THE PRIVACY BAILOUT: STATE GOVERNMENT INVOLVEMENT IN THE PRIVACY ARENA

COREY A. CIOCCHETTI*

I. PREFACE & BACKGROUND

Today's relationship between government and business is more intimate than most Americans prefer.[1] This intermingling intensified as the United States economy faltered in late 2007.[2] The reasons underlying the transformation are as extraordinary as they are tragic. From 2002 to 2007, the world experienced a "global boom."[3] The multitude of economic

---

* Associate Professor of Business Ethics and Legal Studies, University of Denver Daniels College of Business. Please feel free to contact Professor Ciocchetti with updates, questions and comments at cciocche@du.edu. Thanks to the Ohio State University Moritz College of Law and the *Entrepreneurial Business Law Journal* for generously inviting me to present these thoughts at the March 2010 *The Relationship Between American Government and American Business* symposium.

[1] *See, e.g.*, Frank Newport, *Americans More Likely to Say Government Doing Too Much*, GALLUP (Sept. 21, 2009), http://www.gallup.com/poll/123101/americans-likely-say-government-doing-too-much.aspx. Stating that:

> Americans are more likely today than in the recent past to believe that government is taking on too much responsibility for solving the nation's problems and is over-regulating business. New Gallup data show that 57% of Americans say the government is trying to do too many things that should be left to businesses and individuals, and 45% say there is too much government regulation of business. Both reflect the highest such readings in more than a decade.

Id.

[2] Interestingly, the Great Recession is not the only time in American history where the government has been closely involved with business in the form of bailouts although historical bailouts pale in comparison to the total dollar amount of Great Recession bailouts. *See, e.g.*, Jesse Nankin et al., *History of U.S. Gov't Bailouts*, PROPUBLICA.ORG, Apr. 15, 2009, http://www.propublica.org/special/government-bailouts.

[3] *See, e.g.*, Sher Verick & Iyanatul Islam, *The Great Recession of 2008–2009: Causes, Consequences and Policy Responses*, INST. FOR THE STUDY LAB. (Discussion Paper No. 4934, 2010), http://ftp.iza.org/dp4934.pdf. Verick and Islam state that:

> [T]he 2002–2007 period stands out as a case of an unsustainable boom. There was a surge in various forms of external finance (export revenues, remittances, private capital flows) that fed a

success stories enticed the United States government, in combination with real estate interests, to encourage widespread home ownership. Federal action, such as:

1. Expansive interpretations of the Community Reinvestment Act;[4]
2. Increased risk-taking (including one prominent accounting scandal) involving government-sponsored entities such as Fannie Mae and Freddie Mac;
3. An easy monetary policy,[5]

combined with rampant greed from the private sector to contribute to decreased credit-qualification standards and loose lending practices.[6] This

---

> consumption boom in advanced economies and a surge in investment and exports in the developing world led by China and other emerging economies. Overall, the increase in credit flows pushed the cost of capital down. Such a growth experience bred a sense of robust optimism about the future, especially among investors in developed economies leading to an underestimation of risk. This state of mind perhaps contributed to the collective complacency of policymakers, development practitioners and multilateral agencies that were evident even at a time when the seeds of a rather severe global economic recession were being sown in the US heartland.

Id. at 10–11.

[4] *See, e.g.*, John Carney, *Three Ways the CRA Pushed Countrywide to Lower Lending Standards*, BUS. INSIDER, June 25, 2009, http://www.businessinsider.com/three-ways-the-cra-pushed-countrywide-to-lower-lending-standards-2009-6 (providing reasons why the Community Reinvestment Act (CRA), although it was only a major factor in approximately six percent of all sub-prime loans, was a cause of the Great Recession. These reasons include: (1) the creation of artificial demand for low-income mortgages, (2) the threat of regulation is often as good as regulation, and (3) the CRA distorted the mortgage market.).

[5] *See, e.g.*, *Monetary Policy During the Recession of 2007–2009*, UNDERSTANDING MKT., May 6, 2009, http://understandingthemarket.com/?p=64. Stating that:

> When it became clear to the Fed that the economy was slowing sharply and that credit markets were in trouble, the Fed took extraordinary action: they cut rates to virtually zero and then announced that they would buy (in addition to the usual short-term Treasuries) longer-term Treasuries and agency mortgage debt. . . . But such a large expansion of the Fed's balance sheet presents an inflationary threat.

Id.

[6] *See, e.g.*, J.D. Foster, *Understanding the Great Global Contagion and Recession*, HERITAGE FOUND., Oct. 22, 2009, http://www.heritage.org/Research/Reports/2009/10/Understanding-the-Great-Global-Contagion-and-Recession (stating that such

"easy money" allowed individuals to purchase homes they could not necessarily afford (especially if times got tough).[7] Times did get tough as sub-prime, adjustable rate mortgages hit their triggers. These foreseeable, yet consciously ignored, obligations increased monthly mortgage payments drastically and added pressure on the pre-existing real estate bubble. A cascade of foreclosures by home occupants and real estate investors alike burst the bubble dramatically and caused lenders and financial firms holding mortgage-backed securities to suffer catastrophic losses. Insolvencies spread across the financial and real estate sectors to other industries as companies issued earnings warnings.[8] Speculation surrounding lower than anticipated profits shook the markets while

---

factors were partially responsible for the Great Recession). The major accounting scandal involving Fannie Mae included:

> Manipulation of earnings to reach earnings targets to maximize bonuses to company executives. For example, Franklin Raines, former Fannie Mae chief executive officer and former budget director under President Bill Clinton, was forced to pay a $24.7 million fine and give up $15.6 million in stock options for his role in the scandal.

Id.

[7] Peter J. Wallison & Edward J. Pinto, Commentary, *A Government-Mandated Housing Bubble*, FORBES.COM, Feb. 16, 2009, http://www.forbes.com/2009/02/13/housing-bubble-subprime-opinions-contributors_0216_peter_wallison_edward_pinto.html. Wallison and Pinto state that:

> The low interest rates of the early 2000s may explain the growth of the housing bubble, but they don't explain the poor quality of these mortgages. For that we have to look to the government's distortion of the mortgage finance system through the Community Reinvestment Act and the government-sponsored enterprises (GSEs) Fannie Mae and Freddie Mac. In a recent meeting with the Council on Foreign Relations, Barney Frank— the chair of the House Financial Services Committee and a longtime supporter of Fannie and Freddie— admitted that it had been a mistake to force homeownership on people who could not afford it. Renting, he said, would have been preferable . . . . Long-term pressure from Frank and his colleagues to expand home ownership connects government housing policies to both the housing bubble and the poor quality of the mortgages on which it is based.

Id.

[8] *See, e.g.*, Yadav K. Gopalan, *Earliest Indicator of Bank Failure is Deterioration in Earnings*, FED. RES. BANK ST. LOUIS, Spring 2010, http://www.stlouisfed.org/publications/cb/articles/?id=1931 (stating that, "[i]n conclusion, while weakened or deteriorating asset quality is the primary driver of bank stress, the recognition of this stress has historically first shown up in earnings performance").

prodding consumer confidence and spending to retreat.[9] Lower spending hurt bottom lines, and layoffs, downsizing and unemployment followed. By the end of 2009, the Great Recession was in full force.[10]

As conditions worsened, the federal government faced the dilemma of: (1) bailing out imminently insolvent companies deemed by some to be "too big to fail" or (2) allowing such institutions to fail and dealing with the consequences. For the most part, executive officials serving in both the Bush and Obama administrations huddled with Congress and chose the bailout route.[11] As a result, the federal government is closely involved—with mixed results and popularity—in arenas as diverse as Wall Street,[12]

---

[9] *See, e.g., The Dow Jones Industrial Average: December 31, 1974–September 30, 2010*, PRIVATEER, Sept. 30, 2010, http://www.the-privateer.com/chart/dow-long.html (showing the Dow Jones Industrial Average dropped significantly and quickly beginning in late 2007; more specifically, the Dow dropped from 14,164 on October 9, 2007 (a new all-time high) to 7062 on February 27, 2009).

[10] Jacob Weisberg, *What Caused the Great Recession?*, NEWSWEEK, Jan. 9, 2010, at 19.

[11] *See, e.g., Global Financial and Economic Crises 2007-2009*, HIST. COMMONS, http://www.historycommons.org/timeline.jsp?financial_crisis_other=financial_crisis_bailouts&timeline=financial_crisis (showing, in an open-content editing format, the major events of the Great Recession–including the government bailouts–in a timeline format).

[12] *See, e.g., TARP Martyrs: The Political Price of a Good Policy*, WASH. POST, July 5, 2010, at A12. Stating that it is:

> [A]lmost time to say goodbye to the Troubled Assets Relief Program (TARP), the $700 billion bailout fund that pretty much everyone hated, even though it arguably saved the U.S. economy. Unable to win Republican support for their plan to pay for the financial reform bill with a tax on big banks, Democratic leaders in Congress opted to get the cash by closing down TARP now, three months ahead of its scheduled October 3 sunset. For accounting reasons, this frees up $11 billion. It won't affect the Treasury Department's ability to respond to any new crises, which probably would have required additional legislation anyway. Thus ends the much-maligned "Wall Street bailout." It spent or committed only $475 billion of the authorized $700 billion and turned a profit on the capital it provided the banks. Its much-less-than-expected net costs—now $105 billion—are accounted for by mortgage aid to homeowners and the bailouts of the auto industry and insurer AIG.

Id. But see Robert Reich, *The Continuing Disaster of Wall Street, One Year Later*, HUFFINGTON POST, Sept. 14, 2009, http://www.huffingtonpost.com/robert-reich/the-continuing-disaster-o_b_285578.html. Reich states:

> The mega-bailout of Wall Street accomplished little. The only big winners have been top bank executives and traders, whose pay packages are once again in the stratosphere. Banks have been so eager to lure and keep top deal makers and traders

automobiles[13] and environmental cleanup.[14] More specifically, the United States made commitments of $23.9 trillion in bailout funds,[15] faces a

---

> they've even revived the practice of offering ironclad, multimillion-dollar payments—guaranteed no matter how the employee performs.

Id.

[13] *See, e.g.*, KDakotaFund, *Ten Reasons Why the Auto Bailout is a Bad Idea*, MOTLEY FOOL BLOGS (Nov. 22, 2008, 1:00 PM), http://caps.fool.com/Blogs/ten-reasons-why-the-auto/112602; *see also* Ken Dilanian, *Obama Lauds Good News from Auto Industry*, L.A. TIMES, Apr. 25, 2010, at A12. Stating that:

> The auto bailout was less popular [than the recently passed financial regulation bill]. Sixty-one percent opposed it in a CNN/Opinion Research Corp. poll in December 2008. But [President] Obama said Saturday that the auto bailout was "absolutely necessary," because GM and Chrysler were on the brink of collapse. "The best estimates are that more than 1 million American workers could have lost their jobs," he said. At the time, analysts put the cost of the bailout at as high as $130 billion, but the Treasury Department said this week that it would be closer to $28 billion.

Id.

[14] *See, e.g.*, *The Federal Government's Role in BP Oil Spill* (NPR radio broadcast May 25, 2010), *available at* http://www.npr.org/templates/story/story.php?storyId=127114635 (focusing on the oil spill in the Gulf of Mexico and discussing the idea that state and local officials are complaining that "the Obama administration is too slow in channeling supplies and support to protect the fragile coast [and the fact that] an Interior Department inspector general report describes the inappropriate behavior of federal regulators overseeing the drilling."). Also consider:

> BP has correctly received most of the blame for the Deepwater Horizon oil spill. As the contractor of the rig, there is little question that BP is responsible for the accident. However, reports of federal regulatory exemptions and passed safety inspections should raise questions about the federal government's responsibility and the role of regulation . . . As the owner of the waters where drilling takes place, the federal government bears ultimate responsibility for what happens on its property. Even though it leases the space to private investors, it is the government that is responsible for protecting public health, safety, and interests while allowing access to a needed resource through its regulatory authority. Because the federal government exercises significant oversight, it shares some liability for what takes place under the lease.

Jack Spencer, *Gulf Coast Oil Spill: Does the Federal Government Share Responsibility?*, HERITAGE FOUND., May 12, 2010, http://www.heritage.org/research/reports/2010/05/gulf-coast-oil-spill-does-the-federal-government-share-responsibility.

national debt pegged recently at over $13 trillion and budgets under a deficit that hovers around $1.4 trillion.[16] Some people attribute this massive government involvement in business as the reason the United States averted a second Great Depression.[17] Others cower at the record sums of money being spent and the idea that federal employees currently help execute business models they know little about.[18] As optimists begin to reemerge and proclaim that the economy is on the mend,[19] and certain industries start to recruit new talent,[20] these remain tumultuous times for the United States.[21]

---

[15] *See, e.g.*, OFFICE OF THE SPECIAL INSPECTOR GEN. FOR THE TROUBLED ASSET RELIEF PROGRAM, QUARTERLY REPORT TO CONGRESS 3–4 (July 2009). Stating that as:

> Massive and as important as TARP is on its own, it is just one part of a much broader Federal Government effort to stabilize and support the financial system. Since the onset of the financial crisis in 2007, the Federal Government, through many agencies, has implemented dozens of programs that are broadly designed to support the economy and financial system. As detailed in Section 3 of this report, the total potential Federal Government support could reach up to $23.7 trillion.

Id.

[16] *See, e.g.*, U.S. DEBT CLOCK, http://www.usdebtclock.org/ (last visited Oct. 25, 2010) (showing that the "debt per taxpayer" currently stands near $120,000).

[17] *See, e.g.*, Mary Williams Walsh, *Drawing Fire, Geithner Backs Rescue of A.I.G.*, N.Y. TIMES, Jan. 27, 2010, at A3 (discussing Secretary Geithner's testimony in front of a United States House of Representatives Committee and stating that the "questioning was heated and sometimes took on the air of a cross-examination as Mr. Geithner said that a collapse of A.I.G. would have been catastrophic and would have put the United States at risk of a Great Depression.").

[18] *See, e.g.*, Jeffrey A. Miron, Commentary, *Bankruptcy, Not Bailout, is the Right Answer*, CNN, Sept. 29, 2008, http://www.cnn.com/2008/POLITICS/09/29/miron.bailout/index.html?iref=allsearch (discussing reasons why bailing-out struggling companies is "a terrible idea").

[19] *See, e.g.*, Stephanie Condon, *Poll: Public's View of the Economy is Improving*, CBSNEWS, May 3, 2010, http://www.cbsnews.com/8301-503544_162-20004000-503544.html (showing that "[f]orty-one percent of Americans now say the economy is improving, up eight points from April and more than at any time during this recession. Just 15 percent think the economy is getting worse, according to the poll, conducted April 28–May 2 [2010].").

[20] *See, e.g.*, Nelson D. Schwartz, *Wall St. Hiring in Anticipation of Recovery*, N.Y. TIMES, July 11, 2010, at A1. Schwartz states:

> While much of the country remains fixated on the bleak employment picture, hiring is beginning to pick up in the place that led the economy into recession–Wall Street. The shift underscores the remarkable recovery of the biggest banks and brokerage firms since Washington rescued them in the fall of 2008, and follows the huge rebound in profits for members of the

II. INTRODUCTION

In the midst of massive government involvement in the financial, real estate and automotive sectors, other important problems linger without sufficient governmental attention. This Article focuses on one area where federal intervention has been particularly absent—the realm of individual privacy in the Information Age. In America, as opposed to the European Union in particular, the government only sporadically involves itself in protecting a person's privacy from the prying eye of sophisticated monitoring technology. The problem is that monitoring in the United States is increasingly powerful and takes many forms. Online, prominent websites collect, store and disseminate a great deal of personally identifying information (PII) without clearly and simply informing users. This is the case even though such notice is cheap and can be effective. Offline technology exists to monitor individuals driving in their vehicles, walking on the street, shopping in the mall, talking on their cell phones and conducting tasks in and around the workplace. This Article focuses on the lack of involvement by the federal government to protect both individuals and their PII from the prying eyes of both state governments and private businesses/employers.

The Catch-22 is that, today, much of this monitoring exists for acceptable purposes. For example, monitoring occurs in part to: (1) protect the public from criminal activity and threats of such activity; (2) create efficient business practices and work environments; (3) protect institutions from legal liability; and (4) comply with internal or external investigations.

> New York Stock Exchange . . . . Since employment bottomed out in February, New York securities firms have added nearly 2,000 jobs, a trend that is also playing out nationwide at financial companies, commodity contract traders and investment firms. Though the figures are small in comparison to overall Wall Street employment, executives, economists and headhunters say they expect the growth to pick up steam in the coming months.

Id.; *see also U.S. Economy Improving Modestly*, REUTERS, June 9, 2010, http://www.reuters.com/article/idUSN0913384720100609. Stating that United States:

> [E]conomic activity continued to improve since the last report across all 12 Federal Reserve districts, although many districts described the pace of growth as 'modest,' . . . . The report . . . showed consumer and business spending picking up and the job market improving slightly, while inflation remained in check.

Id.

[21] *See, e.g.*, Rolfe Winkler & Alexander Smith, *In Deal-Making, Flat is the New Up*, N.Y. TIMES, June 14, 2010, at B2 (stating that the "trouble is that even though the United States economy has stopped contracting, big risks still weigh on the animal spirits of executives. Job growth is anemic and credit markets have had renewed volatility in the wake of Europe's sovereign debt crisis.").

Each of these four reasons is valid, and such monitoring is upheld in most instances by courts as long as it is reasonable. However, as contemporary monitoring technology becomes increasingly sophisticated, monitoring parties are better able to hone in on increasingly private details of people's lives. At this point, monitoring ceases to serve the valid monitoring purposes and moves into the invasion of privacy arena.

Lacking a clear mandate from Congress on how to protect individuals' PII from this technology, state legislatures receive pressure from their constituents to fill the breach—and many state assemblies have legislated accordingly. The results of such rushed experimentation (a bailout in its own right, so to speak) has created a patchwork of state regulation and subsequent judicial precedent which individuals often find hard to decipher and institutions find hard to comply with. This Article discusses how the lack of federal involvement in the personal privacy arena has enhanced state privacy protections surrounding the monitoring of individuals and their PII. Part II very briefly introduces and evaluates federal protections of persons and their identifying information from sophisticated monitoring practices or, more specifically, the lack thereof. This discussion demonstrates why state governments have been forced to bail out the federal government and deal with privacy invasions stemming from excessive monitoring. Part III is rather unique in the literature in this area and forms the heart of the article. This part comprehensively evaluates how state legislation interacts with the institutions most intimately involved in the monitoring of individuals—state governments, businesses and employers. Specific and common monitoring practices are evaluated and categorized in a fifty state survey to demonstrate and synthesize the patchwork nature of state regulation. Part IV concludes that the contemporary situation is problematic—not in its enhanced protection of individual privacy, which is a positive—but in the patchwork of diverse regulations that confuse consumers and excessively reduce business/employment efficiency. This part concludes with a summary of the current situation and a call for the federal government to reverse the bailout by individual states and begin to formulate national standards for information privacy protection.

III. FEDERAL GOVERNMENT AND REGULATION OF EMPLOYEE PRIVACY

As identified in the preface, the federal government has been understandably distracted over the past few years. At the same time, protection of individual privacy and personally identifying information has suffered from at least a decade of neglect. The problem grows more serious as invasions become more hostile and complex. Invasions become more hostile and complex as contemporary monitoring technology becomes

increasingly sophisticated and institutions begin to implement it ubiquitously.[22] Even though Congress is aware of these invasions and the privacy problem in general, federal law does little to comprehensively protect an individual's privacy and private information.[23] When Congress has chosen to act, it has legislated in a patchwork fashion covering one or two industry sectors at a time.[24] In addition, some privacy protection laws are extremely outdated and not structured to keep up with evolving technology. The Electronic Communications Privacy Act (ECPA), for example, hails from 1986.[25] Today, nearly fifteen years of technological advances have overcome the law's prohibitions and rendered the statute much weaker than it was designed to be. Although "Congress enacted the Electronic Communications Privacy Act of 1986 to protect electronic communications . . . [c]ase law interpreting ECPA is virtually uniform in finding that employers can monitor with or without consent, even without notice."[26] In the end, this is a topic that has been discussed at length in the literature and is not necessary to rehash in this section.[27]

---

[22] *See, e.g.*, *Products Overview*, ALERTSITE, http://www.alertsite.com/product_overview.shtml (last visited Aug. 5, 2010) (showing the many advanced technologies used to potentially monitor individuals).

[23] There are many privacy advocates in the United States who spend a great deal of time and energy making the public—and Congress in particular—aware of contemporary privacy invasions from powerful monitoring technology. *See, e.g.*, *Workplace Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/workplace/ (last visited Aug. 5, 2010).

[24] For examples of federal laws that take an industry-sector approach to protecting privacy, see Privacy Act of 1974, 5 U.S.C. § 552a (2006) (providing individuals with rights concerning their personal information in government records systems); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681t (2006) (providing citizens with rights regarding the use and disclosure of their personal information by credit reporting acts); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2006) (protecting the privacy of school records); Video Privacy Protection Act of 1991, 47 U.S.C. § 227 (2006) (protecting the privacy of videotape rental information); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2006) (mandating privacy protection for records maintained by cable companies). *See also* Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 144 n.51 (2006).

[25] 18 U.S.C. §§ 2510–2521 (2001).

[26] Joan T.A. Gabel & Nancy R. Mansfield, *The Information Revolution and its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace*, 40 AM. BUS. L.J. 301, 315 (2003).

[27] *See* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 22–25 (1st ed. 2003) (providing a very good discussion of privacy law at the federal level); James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 4–5 (2005) (discussing federal privacy law).

Focusing more on the employment front, the primary Catch-22 rests within the employment relationship itself. The vast majority of states (all except Montana) adhere to the employment-at-will theory, which claims that employers have mostly free reign in making decisions concerning their employees.[28] This theory has historically encompassed the idea that employers can monitor the activities of their employees as long as such monitoring is not illegal or does not invade an employee's reasonable expectation of privacy. Today, readily available and increasingly sophisticated monitoring technology provides management with the ability to learn intimate details of their employees' lives and activities. Employers are generally able to show that their monitoring techniques are legal (due to a lack of applicable regulation) and/or that their employees had no reasonable expectation of privacy (due to the fact that the monitoring occurs on employer property, with employer equipment and/or during work hours). On the other hand, courts have held that "while privacy expectations may be significantly diminished in the workplace, they are not lacking altogether."[29] This tension between employer efficiency and employee privacy requires the immediate attention of the federal government as well. Again, this is a topic well covered in the legal literature and will not be rehashed here.[30] The heart of the Article occurs next, in Part IV, and identifies, synthesizes and evaluates a topic that is little discussed in the literature—the protections for individual privacy and PII analyzed on a state by state basis.

IV. STATE GOVERNMENT AND REGULATION OF EMPLOYEE PRIVACY

Individuals are more likely to get results (or at least attention) at the state and local level. It is much easier to get in touch with a state representative or city councilperson than a United States Senator. Feeling the pressure from constituents and suffering from a lack of clear direction from Congress, state officials have involved themselves rather intimately in the privacy arena. This process has produced a patchwork of state laws and legal precedent that might, in the long run, make matters worse. Many of the problems are caused by the following situations: (1) some states seem to copy statutes verbatim from related provisions in existence in state or federal law; (2) while other states harden their stance in an effort to protect PII at great expense to its collectors; (3) while the rest create softer PII protection in comparison or merely ignore the PII protection evolving

---

[28] *See, e.g.*, Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. REV. 331, 338 (2010).

[29] *See* Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1074 (Cal. 2009).

[30] *See, e.g.*, Levinson, *supra* note 28, at 337 n.18 (canvassing the literature and stating that the "lack of adequate protections for employees' right to privacy from employer technological monitoring has been well documented by numerous scholars.").

around the country; and finally (4) some states do all of the above depending upon the particular form of monitoring. The following chart depicts the problem in great detail and is as accurate as possible considering the camouflaged nature of some state privacy protections and the lack of a standardized and comprehensive source to draw from in the literature. The areas covered range from state constitutional protections of privacy to security breach notification laws. This chart—and this Article in general—attempts to fill this gap.

CHART I - STATE LEGISLATION PROPOSED OR ENACTED

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
CONSTITUTIONAL RIGHT TO PRIVACY: APPLIES BROADLY		CALIFORNIA CONSTITUTION (CAL. CONST. art. I, § 1)
CONSTITUTIONAL RIGHT TO PRIVACY: APPLIES TO STATE ACTION ONLY		NINE STATES INCLUDING: ALASKA (ALASKA CONST. art. I, § 22) ARIZONA (ARIZ. CONST. art. II, § 8) FLORIDA (FLA. CONST. art. I, §§ 12, 23) HAWAII (HAW. CONST. art. I, §§ 6, 7) ILLINOIS (ILL. CONST. art. I, §§ 6, 13) LOUISIANA (LA. CONST. art. I, § 5) MONTANA (MONT. CONST. art. II, § 10) SOUTH CAROLINA (S.C. CONST. art. I, § 10) WASHINGTON (WASH. CONST. art. I, § 7)

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
MONITORING IN PRIVATE PLACES BANNED BY STATE LEGISLATION		TWENTY-FOUR STATES INCLUDING: ALABAMA (ALA. CODE § 13A-11-33 (2010)) ARIZONA (ARIZ. REV. STAT. ANN. § 13-3019(A)(1) (2010)) ARKANSAS (ARK. CODE ANN. § 5-16-101(a) 2010)) *CALIFORNIA (CAL. PENAL CODE § 632 (West 2010)) CONNECTICUT (CONN. GEN. STAT. ANN. § 31-48b (2010)) **DELAWARE (DEL. CODE ANN. tit. 11, § 1335(a)(6) (2010)) GEORGIA (GA. CODE ANN. § 16-11-62(2) (2010)) HAWAII (HAW. REV. STAT. §§ 711-1110.9, 711-1111(1)(d)-(e), (g) (2010)) ILLINOIS (720 ILL. COMP. STAT. ANN. 5/26-4(a) (2010)) KANSAS (KAN. STAT. ANN. § 21-4001 (2009)) ***LOUISIANA (LA. REV. STAT. ANN. § 14:283 (2010)) MAINE (ME. REV. STAT. ANN. tit. 17-A, § 511(1)(B) (2010)) MARYLAND (MD. CODE ANN., CRIM. LAW §§ 3-901 to -902 (LexisNexis 2010)) MICHIGAN (MICH. COMP. LAWS ANN. § 750.539(d) (2010)) MINNESOTA (MINN. STAT. ANN. § 609.746(1)(c)-(d) (2010)) MISSOURI (MO. STAT. § 565.253 (2010)) ****NEVADA (NEV. REV. STAT. ANN. § 200.650 (West 2010)) NEW HAMPSHIRE (N.H. REV. STAT. ANN. § 644:9(I)(b)-(c) (2010)) NEW YORK (N.Y. PENAL LAW § 250.45 (McKinney 2010)) ****NORTH DAKOTA (N.D. CENT. CODE § 12.1-15-02(2) (2010)) SOUTH CAROLINA (S.C. CODE ANN. § 16-17-470(A) (2009)) SOUTH DAKOTA (S.D. CODIFIED LAWS § 22-21-1 (2010)) ***TENNESSEE (TENN. CODE ANN. § 39-13-607 (West 2010)) UTAH (UTAH CODE ANN. § 76-9-402 (LexisNexis 2010)) *CONFIDENTIAL COMMUNICATION REQUIRED **ONLY APPLIES TO PLACES WHERE PEOPLE DISROBE AND HAVE A REASONABLE EXPECTATION OF PRIVACY *** RECORDINGS IN ANY PLACE BUT MUST BE MADE FOR LEWD, LASCIVIOUS OR SEXUAL PURPOSES ****PRIVATE PLACE NOT REQUIRED
NOTICE OF ELECTRONIC MONITORING REQUIRED	CALIFORNIA (*vetoed*) MASSACHUSETTS NEW YORK PENNSYLVANIA	THREE STATES INCLUDING: *COLORADO (COLO. REV. STAT. § 18-9-305(1) (2009)) CONNECTICUT (CONN. GEN. STAT. ANN. § 31-48d (2010)) DELAWARE (DEL. CODE ANN. tit. 19, § 705(b)(1)-(2) (2010)) *APPLIES TO WIRETAPPING/EAVESDROPPING DEVICES ONLY
REQUIRED E-MAIL MONITORING POLICY		TWO STATES INCLUDING: *COLORADO (COLO. REV. STAT. § 24-72-204.5 (2009)) *TENNESSEE (TENN. CODE ANN. § 10-7-512 (West 2010)) *APPLICABLE TO STATE EMPLOYERS ONLY

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
INTERCEPTIONS OF ELECTRONIC COMMUNICATIONS: ONLY ONE PARTY NEED CONSENT TO MONITORING		THIRTY-SEVEN STATES INCLUDING: ALABAMA (ALA. CODE § 13A-11-31 (2010)) ALASKA (ALASKA STAT. § 42.20.310 (2010)) ARIZONA (ARIZ. REV. STAT. ANN. § 13-3005(A) (2010)) ARKANSAS (ARK. CODE ANN. § 5-60-120 (2010)) COLORADO (COLO. REV. STAT. ANN. §§ 18-9-303 to -304 (2009)) DELAWARE (DEL. CODE ANN. tit. 11, § 2402(A)(1) (2010)) GEORGIA (GA. CODE ANN. §§ 16-11-62(1), 16-11-66 (2010)) HAWAII (HAW. REV. STAT. § 803-42(b)(3)(A) (2010)) IDAHO (IDAHO CODE ANN. § 18-6702 (2010)) INDIANA (IND. CODE § 35-33.5-1-5 (2010)) *IOWA (IOWA CODE §§ 727.8, 808B.2 (2010)) KANSAS (KAN. STAT. ANN. § 21-4002 (2009)) KENTUCKY (KY. REV. STAT. ANN. § 526.010 (West 2009)) LOUISIANA (LA. REV. STAT. ANN. § 15:1303 (2010)) MAINE (ME. REV. STAT. tit. 15, § 710 (2010)) MINNESOTA (MINN. STAT. § 626A.02 (2010)) MISSISSIPPI (MISS. CODE ANN. § 41-29-531 (2010)) MISSOURI (MO. STAT. § 542.402 (2010)) NEBRASKA (NEB. REV. STAT. § 86-290 (2010)) NEW JERSEY (N.J. STAT. ANN. § 2A:156A-3 (West 2010)) NEW MEXICO (N.M. STAT. ANN. § 30-12-1 (2010)) NEW YORK (N.Y. PENAL LAW §§ 250.00, 250.05 (McKinney 2010)) NORTH CAROLINA (N.C. GEN. STAT. § 15A-287 (2010)) NORTH DAKOTA (N.D. CENT. CODE § 12.1-15-02 (2010)) OHIO (OHIO REV. CODE ANN. § 2933.52 (LexisNexis 2010)) OKLAHOMA (OKLA. STAT. tit. 13, § 176.3 (2010)) OREGON (OR. REV. STAT. § 165.543 (2010)) RHODE ISLAND (R.I. GEN. LAWS § 11-35-21(a), (c)(3) (2010)) SOUTH CAROLINA (S.C. CODE ANN. §§ 17-30-20, 17-30-30 (2009)) SOUTH DAKOTA (S.D. CODIFIED LAWS § 23A-35A-20 (2010)) TENNESSEE (TENN. CODE ANN. § 39-13-601 (2010)) TEXAS (TEX. PENAL CODE ANN. § 16.02 (West 2010)) UTAH (UTAH CODE ANN. § 77-23a-4 (LexisNexis 2010)) VIRGINIA (VA. CODE ANN. § 19.2-62 (2010)) WEST VIRGINIA (W. VA. CODE § 62-1D-3 (2010)) WISCONSIN (WIS. STAT. § 968.31 (2010)) WYOMING (WYO. STAT. ANN. § 7-3-702 (2010)) *CONSENTING PARTY MUST BE PRESENT FOR THE COMMUNICATION

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
INTERCEPTIONS OF ELECTRONIC COMMUNICATIONS: ALL PARTIES MUST CONSENT TO MONITORING		TWELVE STATES INCLUDING: CALIFORNIA (CAL. PENAL CODE §§ 631, 632 (West 2010)) CONNECTICUT (CONN. GEN. STAT. § 52-570d (2010)) *FLORIDA (FLA. STAT. § 934.03(2)(d) (2010)) ILLINOIS (720 ILL. COMP. STAT. ANN. 5/14-2(a)(1) (2010)) MARYLAND (MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (LexisNexis 2010)) MASSACHUSETTS (MASS. GEN. LAWS ANN. ch. 272, § 99(B)(4), (C) (2010)) MICHIGAN (MICH. COMP. LAWS § 750.539(c) (2010)) MONTANA (MONT. CODE ANN. § 45-8-213 (2010)) NEVADA (NEV. REV. STAT. §§ 200.620, 707.900 (2010)) NEW HAMPSHIRE (N.H. REV. STAT. ANN. § 570-A:2 (2010)) PENNSYLVANIA (18 PA. CONS. STAT. § 5703 (2010)) WASHINGTON (WASH. REV. CODE § 9.73.030 (2010)) *ONE PARTY CONSENT REQUIRED FOR INTERCEPTIONS IN THE ORDINARY COURSE OF BUSINESS
MONITORING OF EMPLOYEES' POLITICAL EXPRESSIONS CANNOT LEAD TO ADVERSE ACTION		THIRTY STATES INCLUDING: ARIZONA (ARIZ. REV. STAT. ANN. § 23-1501 (2010)) CALIFORNIA (CAL. LAB. CODE § 1102 (West 2009)) COLORADO (COLO. REV. STAT. § 8-2-102 (2009)) CONNECTICUT (CONN. GEN. STAT. § 31-51q (West 2010)) FLORIDA (FLA. STAT. § 104.081 (2010)) IDAHO (IDAHO CODE ANN. § 18-2319 (2010)) IOWA (IOWA CODE § 39A.5 (2010)) LOUISIANA (LA. REV. STAT. ANN. § 23:961 (2010)) MASSACHUSETTS (MASS. GEN. LAWS ch. 149, § 178 (2010)) MICHIGAN (MICH. COMP. LAWS § 423.508 (2010)) MINNESOTA (MINN. STAT. § 211B.07 (2010)) MISSOURI (MO. REV. STAT. § 115.637(6) (2010)) MONTANA (MONT. CODE ANN. § 13-35-226 (2010)) NEBRASKA (NEB. REV. STAT. § 32-1537 (2010)) NEVADA (NEV. REV. STAT. ANN. § 613.040 (2010)) NEW JERSEY (N.J. STAT. ANN. § 19:34-27 (West 2010)) NEW MEXICO (N.M. STAT. ANN. § 3-8-78 (2010)) NEW YORK (N.Y. LAB. LAW § 201-d (McKinney 2010)) OHIO (OHIO REV. CODE ANN. § 3599.06 (LexisNexis 2010)) OREGON (OR. REV. STAT. § 659.785 (2010)) PENNSYLVANIA (25 PA. CONS. STAT. ANN. § 3547 (2010)) RHODE ISLAND (R.I. GEN. LAWS § 17-23-6 (2010)) SOUTH CAROLINA (S.C. CODE ANN. § 16-17-560 (2010)) SOUTH DAKOTA (S.D. CODIFIED LAWS § 12-26-13 (2010)) TENNESSEE (TENN. CODE ANN. § 2-19-134 (2010)) VERMONT (VT. STAT. ANN. tit. 21, § 1726 (2010)) WEST VIRGINIA (W. VA. CODE ANN. § 3-8-12(k) (2010)) WISCONSIN (WIS. STAT. §103.18 (2010)) WYOMING (WYO. STAT. ANN. § 22-26-116 (2010))

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
EMPLOYERS CANNOT TAKE ADVERSE ACTION BASED ON EMPLOYEE OFF-DUTY ACTIVITIES OR EMPLOYEE OFF-DUTY USE OF LAWFUL PRODUCTS	MICHIGAN	NINE STATES BAN DISCRIMINATION BASED ON ANY OFF-DUTY LAWFUL CONDUCT INCLUDING: CALIFORNIA (CAL. LAB. CODE §§ 96(k), 98.6 (West 2010)) COLORADO (COLO. REV. STAT. § 24-34-402.5 (2009)) CONNECTICUT (CONN. GEN. STAT. § 31-51q (2010)) ILLINOIS (820 ILL. COMP. STAT. 55/5 (2010)) MINNESOTA (MINN. STAT. § 181.938 (2010)) *MISSOURI (MO. REV. STAT. § 290.145 (2010)) NEVADA (NEV. REV. STAT. § 613.333 (2010)) NORTH CAROLINA (N.C. GEN. STAT. 95-28.2 (2010)) **TENNESSEE (TENN. CODE ANN. § 50-1-304 (2010)) *ALCOHOL AND TOBACCO ONLY ** NO DISCRIMINATION AGAINST EMPLOYEE USE OF ANY LEGAL AGRICULTURAL PRODUCT TWENTY STATES BAN DISCRIMINATION BASED ONLY ON OFF-DUTY EMPLOYEE TOBACCO USE INCLUDING: ARIZONA (ARIZ. REV. STAT. ANN. § 36-601.01(F) (2010)) CONNECTICUT (CONN. GEN. STAT. ANN. § 31-40s (2010)) INDIANA (IND. CODE § 22-5-4-1 (2010)) KENTUCKY (KY. REV. STAT. ANN. § 344.040 (West 2009)) LOUISIANA (LA. REV. STAT. ANN. § 23:966 (2010)) MAINE (ME. REV. STAT. ANN. tit. 26, § 597 (2010)) MISSISSIPPI (MISS. CODE ANN. § 71-7-33 (2010)) MONTANA (MONT. CODE ANN. § 39-2-313(2) (2010)) NEW HAMPSHIRE (N.H. REV. STAT. ANN. § 275:37-a (2010)) NEW JERSEY (N.J. STAT. ANN. § 34:6B-1 (West 2010)) NEW MEXICO (N.M. STAT. ANN. § 50-11-3 (2010)) NEW YORK (N.Y. LAB. LAW § 201-d(1)(b)–(c) (McKinney 2010)) NORTH DAKOTA (N.D. CENT. CODE § 14-02.4-03 (2010)) OKLAHOMA (OKLA. STAT. tit. 40, § 500 (2010)) OREGON (OR. REV. STAT. § 659A.315 (2010)) SOUTH CAROLINA (S.C. CODE ANN. § 41-1-85 (2009)) SOUTH DAKOTA (S.D. CODIFIED LAWS § 60-4-11 (2010)) WEST VIRGINIA (W. VA. CODE § 21-3-19 (2010)) WISCONSIN (WIS. STAT. § 111.321 (2010)) WYOMING (WYO. STAT. ANN. § 27-9-105(a)(iv) (2010)) *ARIZONA (ARIZ. REV. STAT. ANN. § 36-601-02 (repealed May 1, 2007)) *RHODE ISLAND (R.I. GEN. LAWS § 23-20.7.1-1 (repealed March 1, 2005))

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
RFID DISCLOSURE, RESTRICTION, SECURITY, IMPLANTATION & DEACTIVATION LAWS	FIVE STATES INCLUDING: MASSACHUSETTS NEW MEXICO OHIO RHODE ISLAND TENNESSEE	ELEVEN STATES INCLUDING: CALIFORNIA (CAL. CIV. CODE § 1798.79 (West 2009)) MISSOURI (MO. REV. STAT. § 285.035 (2010)) NEVADA (NEV. REV. STAT. ANN. § 205.46515 (West 2010)) *NEW HAMPSHIRE (N.H. REV. STAT. § 236:130 (2010)) NORTH DAKOTA (N.D. CENT. CODE § 12.1-15-06 (2010)) OKLAHOMA (OKLA. STAT. tit. 63, § 1-1430 (2010)) TEXAS (TEX. TRANSP. CODE ANN. § 521.032 (2010)) VERMONT (VT. STAT. ANN. tit. 23, § 7 (2010)) VIRGINIA (VA. CODE ANN. § 46.2-323.01 (2010)) **WASHINGTON (WASH. REV. CODE § 46.20.202 (2010)) ***WASHINGTON (WASH. REV. CODE §§ 9A.58.020, 19.200.030 (2010)) WISCONSIN (WIS. STAT. ANN. § 146.25 (West 2010)) *RFID TECHNOLOGY BANNED ONLY FOR GOVERNMENTAL USE ON STATE HIGHWAYS TO IDENTIFY VEHICLE OWNERSHIP OR OCCUPANTS ** RFID TECHNOLOGY USED IN STATE ID CARDS MUST BE SECURED ***RFID SKIMMING PROHIBITED
RFID STUDY TASK FORCE CREATED	FOUR STATES INCLUDING: ARKANSAS MARYLAND NEW YORK NEW HAMPSHIRE	
LAWS THAT ENCOURAGE/REQUIRE RFID IN IDENTIFICATION CARDS		TWO STATES INCLUDING: MICHIGAN (MICH. COMP. LAWS § 28.304 (2010)) VERMONT (VT. STAT. ANN. tit. 23, § 7 (2010))

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
GOVERNMENTAL AGENCIES AND/OR BUSINESSES REQUIRED TO CREATE AND POST PRIVACY POLICIES DESCRIBING HOW THE INSTITUTION DEALS WITH PII		TWENTY STATES INCLUDING: *ARIZONA (ARIZ. REV. STAT. ANN. §§ 41-4151 to 4152 (2010)) *ARKANSAS (ARK. CODE ANN. § 25-1-114 (2010)) CALIFORNIA (CAL. BUS. & PROF. CODE § 22575 (West 2009)) *CALIFORNIA (CAL. GOV'T CODE § 11019.9 (West 2009)) *COLORADO (COLO. REV. STAT. §§ 24-72-501 to 502 (2009)) **CONNECTICUT (CONN. GEN. STAT. § 42-471(b) (2010)) *DELAWARE (DEL. CODE ANN. tit. 29, § 9018C (2010)) *IOWA (IOWA CODE § 22.11(1) (2010)) *MARYLAND (MD. CODE ANN., STATE GOV'T § 10-624 (LexisNexis 2010)) **MICHIGAN (MICH. COMP. LAWS § 445.84 (2010)) *MINNESOTA (MINN. STAT. §§ 13.055, 13.15 (2010)) *MONTANA (MONT. CODE ANN. § 2-17-552 (2010)) ***NEBRASKA (NEB. REV. STAT. § 87-302(a)(14) (2010)) *NEW YORK (N.Y. STATE TECH. LAW §§ 203–204 (McKinney 2010)) PENNSYLVANIA (18 PA. CONS. STAT. § 4107(a)(10) (2010)) *SOUTH CAROLINA (S.C. CODE ANN. §§ 30-2-20, 30-2-40 (2009)) **TENNESSEE (TENN. CODE ANN. § 47-18-2110 (2010)) *TEXAS (TEX. GOV'T CODE ANN. § 2054.126 (West 2010)) *UTAH (UTAH CODE ANN. § 63D-2-103 (LexisNexis 2010)) *VIRGINIA (VA. CODE ANN. § 2.2-3803 (2010)) *REQUIRED ONLY FOR STATE GOVERNMENTAL ENTITIES **REQUIRED ONLY IF SSNS ARE COLLECTED ***RELEVANT ONLY IF PRIVACY POLICIES ARE VIOLATED

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
PROHIBITIONS OF GENETIC TESTING/USE OF GENETIC TESTS		THIRTY-FIVE STATES INCLUDING: ALASKA (ALASKA STAT. § 18.13.010 (2010)) ARIZONA (ARIZ. REV. STAT. ANN. § 41-1463 (2010)) ARKANSAS (ARK. CODE ANN. §§ 11-5-401 to -405 (2010)) CALIFORNIA (CAL. GOV'T CODE §§ 12926, 12940 (West 2010)) CONNECTICUT (CONN. GEN. STAT. § 46a-60 (2010)) DELAWARE (DEL. CODE ANN. tit. 19, §§ 710–711 (2010)) HAWAII (HAW. REV. STAT. §§ 378-1 to -10 (2010)) IDAHO (IDAHO CODE ANN. §§ 39-8301 to -8304 (2010)) ILLINOIS (410 ILL. COMP. STAT. ANN. 513/25; 215 ILL. COMP. STAT. ANN. 5/356v (2010)) IOWA (IOWA CODE § 729.6 (2010)) KANSAS (KAN. STAT. ANN. § 44-1002 (2010)) LOUISIANA (LA. REV. STAT. ANN. § 23:302 (2010)) MAINE (ME. REV. STAT. tit. 5, § 19302 (2010)) MARYLAND (MD. CODE ANN., HUM. REL. COMM'N CODE § 49B-15 (LexisNexis 2010)) MASSACHUSETTS (MASS. GEN. LAWS ch. 151b, § 4 (2010)) MICHIGAN (MICH. COMP. LAWS § 37.1201 (2010)) MINNESOTA (MINN. STAT. ANN. § 181.974 (West 2010)) MISSOURI (MO. ANN. STAT. § 375.1300 (West 2010)) NEBRASKA (NEB. REV. STAT. § 48-236 (2010)) NEVADA (NEV. REV. STAT. § 613.345 (2010)) NEW HAMPSHIRE (N.H. REV. STAT. ANN. § 141-H:1 (2010)) NEW JERSEY (N.J. STAT. ANN. § 10:5-5 (West 2010)) NEW MEXICO (N.M. STAT. ANN. § 24-21-7 (2010)) NEW YORK (N.Y. EXEC. LAW § 292 (McKinney 2010)) NORTH CAROLINA (N.C. GEN. STAT. § 95-28.1A (2010)) OKLAHOMA (OKLA. STAT. tit. 36, § 3614.2 (2010)) OREGON (OR. REV. STAT. § 659A.300 (2010)) RHODE ISLAND (R.I. GEN. LAWS § 28-6.7-1 (2010)) SOUTH DAKOTA (S.D. CODIFIED LAWS § 60-2-20 (2010)) TEXAS (TEX. LAB. CODE ANN. § 21.402 (West 2010)) UTAH (UTAH CODE ANN. § 26-45-103 (LexisNexis 2010)) VERMONT (VT. STAT. ANN. tit. 18, § 9333 (2010)) VIRGINIA (VA. CODE ANN. § 40.1-28.7:1 (2010)) WASHINGTON (WASH. REV. CODE § 49.44.180 (2010)) WISCONSIN (WIS. STAT. § 111.372 (2010))

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
GOVERNMENTAL AGENCY AND/OR BUSINESS REQUIRED TO PROTECT PERSONALLY IDENTIFYING INFORMATION		TEN STATES INCLUDING: ALASKA (ALASKA STAT. §§ 45.48.010–.100 (2010)) ARIZONA (ARIZ. REV. STAT. ANN. §§ 44-7501, 7601 (2010)) *ILLINOIS (5 ILL. COMP. STAT. 179/37 (2010)) *MARYLAND (MD. CODE ANN., COM. LAW § 14-3402 (LexisNexis 2010)) *NORTH CAROLINA (N.C. GEN. STAT. § 132-1.10 (2010)) RHODE ISLAND (R.I. GEN. LAWS § 11-49.2-2(2) (2010)) SOUTH CAROLINA (S.C. CODE ANN. § 30-2-310 (2009)) *SOUTH CAROLINA (S.C. CODE ANN. § 37-20-180 (2009)) TENNESSEE (TENN. CODE ANN. § 47-18-2110 (2010)) *TEXAS (TEX. BUS. & COM. CODE ANN. § 501.052 (West 2010)) VIRGINIA (VA. CODE ANN. § 2.2-3808 (2010)) *TARGETED TOWARDS USE OF SOCIAL SECURITY NUMBERS ONLY
PROTECTION AGAINST SALES AND/OR OTHER DISSEMINATION OF PII		SEVEN STATES INCLUDING: CALIFORNIA (CAL. CIV. CODE §§ 1798.83– .84 (West 2009)) MINNESOTA (MINN. STAT. §§ 13.055, 13.15 (2010)) MONTANA (MONT. CODE ANN. § 2-17-552(1)–(3) (2010)) *NEW YORK (N.Y. STATE TECH. LAW § 204 (McKinney 2010)) RHODE ISLAND (R.I. GEN. LAWS § 11-49.2-2(3) (2010)) SOUTH CAROLINA (S.C. CODE ANN. § 30-2-320 (2009)) UTAH (UTAH CODE ANN. § 13-37-201 (LexisNexis 2010)) *APPLICABLE TO STATE AGENCIES ONLY

SUBJECT OF STATE LEGISLATION	PROPOSED IN:	ENACTED IN:
SECURITY BREACH INVESTIGATION AND NOTIFICATION REQUIREMENTS	MISSISSIPPI	FORTY-FIVE STATES INCLUDING: ALASKA (ALASKA STAT. § 45.48.010 (2010)) ARIZONA (ARIZ. REV. STAT. ANN. § 44-7501 (2010)) ARKANSAS (ARK. CODE ANN. § 4-110-101 (2010)) CALIFORNIA (CAL. CIV. CODE §§ 56.06, 1785.11.2, 1798.29, 1798.82 (West 2010)) COLORADO (COLO. REV. STAT. § 6-1-716 (2010)) CONNECTICUT (CONN. GEN. STAT. ANN. § 36a-701 (2010)) DELAWARE (DEL. CODE ANN. tit. 6, § 12B-101 (2010)) FLORIDA (FLA. STAT. § 817.5681 (2010)) GEORGIA (GA. CODE ANN. § 10-1-910 (2010)) HAWAII (HAW. REV. STAT. § 487N-2 (2010)) IDAHO (IDAHO CODE ANN. § 28-51-104(2010)) ILLINOIS (815 ILL. COMP. STAT. ANN. § 530/1 (2010)) INDIANA (IND. CODE § 24-4.9 (West 2010)) IOWA (IOWA CODE § 1347.12 (West 2010)) KANSAS (KAN. STAT. ANN. § 1347.12 (2010)) LOUISIANA (LA. REV. STAT. ANN. § 51:3071 (2010)) MAINE (ME. REV. STAT. ANN. tit. 10, § 1346– 1350-A (2010)) MARYLAND (MD. CODE ANN., COM. LAW § 14-3504 (LexisNexis 2010)) MASSACHUSETTS (MASS. GEN. LAWS ch. 93H, § 1–6 (2010)) MICHIGAN (MICH. COMP. LAWS § 445.72 (2010)) *MINNESOTA (MINN. STAT. § 13.055(subdiv. 2) (2010)) MISSOURI (MO. REV. STAT. § 407.1500 (2010)) MONTANA (MONT. CODE ANN. § 30-14-1704(1)– (2) (2010)) NEBRASKA (NEB. REV. STAT. § 87-803 (2010)) NEVADA (NEV. REV. STAT. § 603A.010 (2010)) NEW HAMPSHIRE (N.H. REV. STAT. ANN. § 359-C:20 (2010)) NEW JERSEY (N.J. STAT. ANN. § 56:8-163 (West 2010)) *NEW YORK (N.Y. STATE TECH. LAW § 208 (McKinney 2010)) NEW YORK (N.Y. GEN. BUS. LAW § 899-aa (McKinney 2010)) NORTH CAROLINA (N.C. GEN. STAT. § 75-65 (2010)) NORTH DAKOTA (N.D. CENT. CODE § 51-30-01 (2010)) OHIO (OHIO REV. CODE ANN. § 1347.12 (LexisNexis 2010)) OKLAHOMA (OKLA. STAT. tit. 24, §§ 161–166 (2010)) OREGON (OR. REV. STAT. § 646A.600 (2010)) PENNSYLVANIA (73 PA. CONS. STAT. § 2303 (2010)) **RHODE ISLAND (R.I. GEN. LAWS § 11-49.2-3 (2010)) SOUTH CAROLINA (S.C. CODE ANN. § 39-1-90 (2009)) TENNESSEE (TENN. CODE ANN. § 47-18-2107 (2010)) TEXAS (TEX. BUS. & COM. CODE ANN. § 521.03 (West 2010)) UTAH (UTAH CODE ANN. § 13-44-101 (LexisNexis 2010)) VERMONT (VT. STAT. ANN. tit. 9, § 2430 (2010)) VIRGINIA (VA. CODE ANN. § 18.2–186.6 (2010)) WASHINGTON (WASH. REV. CODE § 19.255.010 (2010)) WEST VIRGINIA (W.VA. CODE § 46A-2A-101 (2010)) WISCONSIN (WIS. STAT. § 134.98 (2010)) WYOMING (WYO. STAT. ANN. §§ 40-12-501, 40-12-502 (2010)) *COVERS GOVERNMENTAL USE OF PII ONLY **COVERS BOTH PRIVATE AND GOVERNMENTAL USE OF PII

A. *Alabama*

1. *Electronic Monitoring & Eavesdropping*

Alabama is not exactly on the privacy-protective end of the spectrum. In fact, Alabama state law only requires one party to a communication to consent to the use of "any device" to overhear or record communications.[31] This is true whether the person monitoring the communication is present or not.[32] Such provisions allow individuals to record their own conversations and employers to covertly monitor their employees. The covert angle provides management with a better chance of keeping records and discovering illegal activity or violations of company policy. On the other hand, covert monitoring of employees in the workplace negatively impacts morale. Without consent, a violation of the statute occurs when "there is (1) a willful interception, (2) of oral communications uttered by a person exhibiting an expectation that the communication would be in private, (3) and communication is made under circumstances justifying an expectation of privacy."[33] Most individuals generally expect that their conversations are private. However, courts will have to decide whether such an expectation is, in fact, reasonable. The Alabama code also criminalizes eavesdropping when a person "intentionally installs or places a device in a private place with knowledge it is to be used for eavesdropping and without permission of the owner and any lessee or tenant or guest for hire of the private place."[34] This prohibition would not likely preclude employers from placing eavesdropping devices in the workplace because management generally has the "permission of the owner" and the vast majority of the areas within workplaces are not generally considered private places. It would ban eavesdropping in restrooms, locker rooms, etc.

2. *Statutory Right to Privacy*

Tangentially, the Alabama Mental Health Consumers' Rights Act (MHCRA) creates an interesting situation which might be construed to provide individuals (and potentially employees) with additional privacy protections. The MHCRA states that consumers "of mental health services have *the same general rights as other citizens of Alabama.* These rights include but are not limited to the following . . . [i]n residential or inpatient programs, *the right to privacy.*"[35] It is possible, but perhaps unlikely, that

---

[31] ALA. CODE § 13A-11-31 (2010).
[32] *Id.*
[33] Ages Group, L.P. v. Raytheon Aircraft Co., Inc., 22 F. Supp. 2d 1310, 1320 (M.D. Ala. 1998).
[34] ALA. CODE § 13A-11-33(a) (2010).
[35] *Id.* § 22-56-4(a), (b)(18) (emphasis added). The Alabama Code also makes a similar statement concerning persons with developmental disabilities and traumatic

Alabama courts might interpret this provision broadly and transfer its meaning to protect employee privacy in the workplace.

B. *Alaska*

1. *Constitutional Protection*

Alaska's constitution states that "[t]he right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."[36] Problematically, the Alaska state legislature has struggled to clarify this privacy language.[37] The Alaska courts have held that the provision does not apply without state action depriving an individual of privacy.[38] These holdings are based on an analysis of voter intent at the time the provision was enacted. The Alaska Supreme Court held that voters must clearly intend for the right to privacy to apply to private actors and that this was not the case with Article I, Section 22.[39]

---

brain injuries. *Id.* § 38-39C-4(11) (stating that the "rights of persons with developmental disabilities and traumatic brain injury include, but are not limited to, all of the following . . . [t]he right to privacy and dignity.").

[36] ALASKA CONST. art. I, § 22.

[37] *See, e.g.*, Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1129 (Alaska 1989). Stating that:

> We observe initially that this provision, powerful as a constitutional statement of citizens' rights, contains no guidelines for its application. Nor does it appear that the [Alaska] legislature has exercised its power to apply the provision; the parties did not bring to our attention any statutes which "implement this section.

Id.

[38] For instance, a grocery store clerk at an Alaska Safeway was terminated for failing to cut his hair under the company's grooming policy. Miller v. Safeway, Inc., 102 P.3d 282, 284 (Alaska 2004) (stating the pertinent facts of the case as follows: "Frank Miller [an Alaska Native] was terminated from his employment at Safeway after he refused to cut his hair in accordance with a corporate grooming policy. He sued on the grounds that the policy discriminated on the basis of race, religion, and gender, *and that it violated his right to privacy.*") (emphasis added). In his subsequent lawsuit, the Alaska court held that this policy by a private employer did not constitute state action and, thus, the privacy protection of the state constitution was inapplicable. *Id.* at 290 (holding that the plaintiff-employee "has failed to produce evidence that the [Alaska] voters who ratified Section 22 specifically intended that the privacy amendment should apply to private action. Thus, the superior court did not err in its determination that state action is required to assert a violation of a constitutional right to privacy.").

[39] *Id.* at 290. In *Miller*, the Alaska Supreme Court held that "Safeway convincingly [argued] that the citizens who ratified the amendment voted on a version of Section 22 that did not contain any specific language regarding penalties for private action." *Id.*

2 *Electronic Monitoring & Eavesdropping*

Alaska statutory law does not offer much protection from sophisticated monitoring technology. Employers may audiotape employees without gaining their consent, as Alaska law only requires one party to the conversation to consent.[40] The Alaska Supreme Court held that the eavesdropping statute was "intended to prohibit third-party eavesdropping and is therefore not applicable [to a participant in a conversation]."[41] It is a crime in Alaska to view or produce a picture of a naked or partially naked person without consent.[42] This might pose an issue to employers desiring to record employee actions in restrooms or locker rooms in a theft investigation, etc. However, "[i]n a prosecution under this section, it is an affirmative defense that the viewing or photography was conducted as a security surveillance system, notice of the viewing or photography was posted, and any viewing or use of pictures produced is done only in the interest of crime prevention or prosecution."[43]

3. *Miscellaneous Privacy Protection*

The code does prohibit one form of employee monitoring using sophisticated technology—the use of genetic testing on individuals without "informed and written consent."[44] Finally, a new Alaska law protects privacy in personally identifying information (PII) both inside and outside of the workplace. The new Personal Information Protection Act requires businesses to notify consumers when their PII is accessed inappropriately, allows individuals to place freezes on their credit reports and scores, restricts the use of social security numbers and requires businesses to take

---

[40] ALASKA STAT. § 42.20.310 (2010).

[41] Palmer v. State, 604 P.2d 1106, 1108 n.5 (Alaska 1979); *see also* THE REPORTERS COMM. FOR FREEDOM OF THE PRESS, CAN WE TAPE? at Alaska (Fall 2008) [hereinafter CAN WE TAPE?] (citing *Palmer*, 604 P.2d 1106).

[42] ALASKA STAT. § 11.61.123 (2010).

[43] *Id.* § 11.61.123(d).

[44] *Id.* § 18.13.010(a)(1)–(2). Stating that:

> Except as provided . . . (1) a person may not collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis unless the person has first obtained the informed and written consent of the person, or the person's legal guardian or authorized representative, for the collection, analysis, retention, or disclosure; (2) a DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled or analyzed.

Id.

care to protect PII when disposing of records.[45] These types of protections of PII indicate that the Alaska state legislature is at least aware of the invasiveness of contemporary technology. The next step in such protection could encourage legislation designed to beef up privacy in the workplace.

C. *Arizona*

1. *Constitutional Protection*

Arizona's constitution states: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law."[46] Similar to Alaska—and nine of the ten state constitutions mentioned in this section—this provision only applies to invasions of privacy by state actors. Arizona courts have held that the provisions "was not intended to give rise to a private cause of action between private individuals, but was intended as a prohibition on the State and has the same effect as the Fourth Amendment of the Constitution of the United States."[47] Backing up this idea is the preamble to the Arizona Employment Protection Act, which "was intended to eliminate judicial discretion in determining whether a plaintiff has alleged a violation of public policy in a wrongful termination suit."[48] More specifically, the Arizona legislature declared that "public policy is expressly determined by the legislature in the form of statutory provisions [and that the Arizona Constitution] did not intend to vest the courts with the authority to establish . . . the public policy of the state."[49] This legislative intent might skew future interpretations of Arizona's constitutional right to privacy away from limiting monitoring as courts leave it to the legislature to specifically protect employee privacy.

---

[45] *Id.* §§ 45.48.010–.995. The state also protects workers compensation records by classifying them as not public. *Id.* § 23.30.107(b) (stating that, "[m]edical or rehabilitation records, and the employee's name, address, social security number, electronic mail address, and telephone number contained on any record, in an employee's file maintained by the division or held by the board or the commission are not public records subject to public inspection and copying").

[46] ARIZ. CONST. art. II, § 8.

[47] Cluff v. Farmers Ins. Exch., 460 P.2d 666, 669 (Ariz. Ct. App. 1969); *see also* Amor v. Arizona, No. CIV 06-499-TUC-CKJ, 2009 WL 529326, at *93 (D. Ariz. Feb. 27, 2009) (citing *Cluff* and holding that Arizona's constitutional right to privacy was not "intended to give rise to a private cause of action between private individuals. The court having found that [the doctor who was the defendant in the case] is not a state actor, the court finds Amor has failed to state a claim against [the defendant] under [the Arizona Constitution].").

[48] Aaron C. Schepler, Note, Comments and Legislative Review: Hart v. Seven Resorts, Inc.: *Should the Arizona Constitution Protect Employees from Employer-Mandated Drug Testing?*, 30 ARIZ. ST. L.J. 541, 555–56 (1998).

[49] *See* 1996 Ariz. Sess. Laws, ch. 140, 1(A).

2. *Electronic Monitoring & Eavesdropping*

Arizona law allows the interception of a wire or electronic conversation of an individual as long as one party to the conversation consents.[50] Employers may also intercept (i.e., eavesdrop upon) a non-electronic conversation in all places where employees do not have a reasonable expectation of privacy.[51] However, it is:

> [U]nlawful for any person to knowingly photograph, videotape, film, digitally record or by any other means secretly view, with or without a device, another person without that person's consent . . . [i]n a restroom, bathroom, locker room, bedroom or other location where the person has a reasonable expectation of privacy and the person is urinating, defecating, dressing, undressing, nude or involved in sexual intercourse or sexual contact . . . ."[52]

The law does not apply to "[p]hotographing, videotaping, filming or digitally recording for security purposes if notice of the use . . . is clearly posted in the location and the location is one in which the person has a reasonable expectation of privacy."[53]

3. *Miscellaneous Privacy Protection*

Arizona law bans smoking in the workplace but also prohibits employers from retaliating or terminating an employee after discovering that such employee smokes in places legally allowed by Arizona law.[54] Arizona law does marginally protect an individual's personal information. The state code requires entities (including businesses) to redact or destroy PII on records before discarding such records.[55] Arizona businesses must

---

[50] ARIZ. REV. STAT. ANN. § 13-3005(A)(1) (2010) (stating that "[e]xcept as provided . . . a person is guilty of a class 5 felony who . . . [i]ntentionally intercepts a wire or electronic communication to which he is not a party, or aids, authorizes, employs, procures or permits another to so do, without the consent of either a sender or receiver thereof.").

[51] *Id.* § 13-3001(8) (defining "oral communication" and allowing the monitoring of oral communications unless the "spoken communication . . . is uttered by a person who exhibits an expectation that the communication is not subject to interception under circumstances justifying the expectation [of privacy].").

[52] *Id.* § 13-3019(A)(1).

[53] *Id.* § 13-3019(C)(1).

[54] *Id.* § 36-601.01(B) (stating that smoking is allowed in Arizona in the places specifically listed in the statute).

[55] *Id.* § 44-7601(A) (stating that PII consists of an individual's first and last name or first initial and last name combined with an individual's complete: (1) Social security number; (2) Credit card, charge card or debit card number; (3) Retirement

also notify affected individuals when an internal investigation indicates that their PII has been compromised.[56] As stated above, protections of PII indicate that the state legislature is at least aware of the invasiveness of contemporary technology.

D. *Arkansas*

1. *Electronic Monitoring & Eavesdropping*

Arkansas allows electronic or oral conversations to be recorded if the person recording the conversation is a party to the conversation or if one person to the conversation consents.[57] Interestingly, Arkansas law states that "[i]f any person without authority intercepts a dispatch or message transmitted by telephone or willfully destroys or injures any telephone pole, wire, cable, or fixture, he or she is guilty of a Class A misdemeanor."[58] This section likely prohibits employers from monitoring the telephone calls of their employees. Arkansas also codified the crime of video voyeurism stating that it:

> [I]s unlawful to use any camera, videotape . . . or any other image recording device for the purpose of secretly observing, viewing, photographing, filming, or videotaping a person present in a residence, place of business, school, or other structure, or any room or particular location within that structure, if that person: is in a private area out of public view; has a reasonable expectation of privacy; and has not consented to the observation.[59]

There is an exception to the law if the security monitoring is "operated by or at the direction of the owner or administrator of a place of business . . . ."[60] This should allow employers to record employees in private areas of the workplace during internal security investigations.

E. *California*

1. *Constitutional Protection*

California's constitutional right to privacy is a different story entirely. This provisions states that "[a]ll people are by nature free and independent

---

account number; (4) Savings, checking or securities entitlement account number; or (5) Driver license number or non-operating identification license number).

[56] *Id.* § 44-7501.

[57] ARK. CODE ANN. § 5-60-120 (2010).

[58] *Id.* § 23-17-107.

[59] *Id.* § 5-16-101(a).

[60] *Id.* § 5-16-101(d)(3).

and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[61] Unlike Alaska's constitutional privacy protection, courts in California consistently hold that this privacy provision does apply to private actors.[62] To prevail in court under the California constitutional right to privacy, an aggrieved individual must:

1. Possess a legally protected privacy interest—which includes, 'conducting personal activities without observation, intrusion, or interference' as determined by 'established social norms' derived from such sources as the 'common law' and 'statutory enactment';[63]
2. Possess a reasonable expectation of privacy—which rests on an examination of 'customs, practices, and physical settings surrounding particular activities,' as well as the opportunity to be notified in advance and consent to the intrusion;[64]
3. Show that the intrusion is so serious in "nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms";[65] and
4. Be able to overcome the employer's defense that a less intrusive means of monitoring was not available.[66]

2. *Especially Relevant Case Law*

Along these lines, this constitutional privacy protection is not unlimited in favor of employees even in California. For example, the California

---

[61] CAL. CONST. art. I, § 1.

[62] *See, e.g.*, Chico Feminist Women's Health Ctr. v. Butte Glenn Med. Soc'y, 557 F. Supp. 1190, 1203 (E.D. Cal. 1983) (holding that "[i]n sum, the court finds that California law supports the conclusion that Article I, § 1 was intended to provide sweeping protection against interference with all personal privacy rights and that such protection was meant to include protection against the acts of private parties"); Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994) (holding that "article I, section 1 of the California Constitution creates a right of action against private as well as government entities. The legal concept of 'privacy' as embodied in the [article] is susceptible of such an interpretation; the ballot arguments strongly support it.").

[63] Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009) (quoted in *Hill*, 865 P.2d at 654).

[64] *Id.*

[65] *Id.* (quoted in *Hill*, 865 P.2d at 655).

[66] *Id.* (citing relevant precedent and stating that a "relevant inquiry in this regard is whether the intrusion was limited, such that no confidential information was gathered or disclosed.").

Supreme Court recently held that employers may place hidden video cameras in particular places for particular reasons and that not all reasonable expectations of privacy are strong enough to completely ban video monitoring on work premises.[67] In *Hernandez v. Hillsides*, an employer suspected that someone was sneaking into the offices of Hillsides employees late at night to view pornography.[68] To catch the suspect in violation of company policy, management installed a camera in an enclosed office shared by two employees—neither of which was informed of the monitoring or suspected of the violation.[69] The camera only recorded activity at night—when the suspected activity was taking place—and never recorded either of the employees who worked in the office.[70] Regardless, when the employees discovered the monitoring, they sued Hillsides for, among other things, violating their state constitutional right to privacy.[71] Hillsides argued that these employees suffered no privacy invasion because they were never videotaped.[72] On the contrary, the employees argued that

---

[67] *See id.* at 1082.

[68] *Id.* at 1066.

> [T]he director of the facility, learned that late at night, after plaintiffs had left the premises, an unknown person had repeatedly used a computer in plaintiffs' office to access the Internet and view pornographic Web sites. Such use conflicted with company policy and with Hillsides's aim of providing a safe haven for the children.

Id.

[69] *Id.* (stating that the director was "concerned that the culprit might be a staff member who worked with the children."). With this in mind and "without notifying plaintiffs, [the director] set up a hidden camera in their office." *Id.*

[70] *Id.*

> The camera could be made operable from a remote location, at any time of day or night, to permit either live viewing or videotaping of activities around the targeted workstation. It is undisputed that the camera was not operated for either of these purposes during business hours, and, as a consequence, that plaintiffs' activities in the office were not viewed or recorded by means of the surveillance system. [The director] did not expect or intend to catch plaintiffs on tape.

Id.

[71] *Id.* ("[A]fter discovering the hidden camera in their office, plaintiffs filed this tort action alleging, among other things, that defendants intruded into a protected place, interest, or matter, and violated their right to privacy under both the common law and the state Constitution.").

[72] *Id.* at 1072. Stating that Hillsides argues:

> [T]hat they did nothing wrong in attempting to videotape a nighttime intruder using the computer in plaintiffs' office, because no private information about plaintiffs was obtained. Defendants insist that plaintiffs, not being the intended targets of the surveillance plan, were never viewed or recorded, and thereby

they had a reasonable expectation of privacy in their closed office and that the placement of the camera itself, with the ability to record them at any time—constituted a privacy violation.[73] The Court held that while the employees did possess a reasonable expectation of privacy in their enclosed office, the video recording that took place in this case was neither highly offensive nor an "egregious breach of the social norms."[74] Therefore, the monitoring did not violate the California Constitution.

The *Hernandez* case made it clear that video monitoring that captured employees actually present in their enclosed offices would violate the California Constitution. In fact, the California Supreme Court sympathized with the plaintiff employees in the case by stating:

> We appreciate plaintiffs' dismay over the discovery of video equipment—small, blinking, and hot to the touch—that their employer had hidden among their personal effects in an office that was reasonably secluded from public access and view. Nothing we say here is meant to encourage such surveillance measures, particularly in the absence of adequate notice to persons within camera range that their actions may be viewed and taped.[75]

> suffered no serious or actionable intrusion into their private domain.

Id.

[73] *Id.* (stating that the employees insisted "that defendants were able to view and record plaintiffs at will, without their knowledge or consent, and unjustifiably deprived them of the privacy they reasonably expected to have while working behind closed doors in their shared office.").

[74] *Id.* at 1082. Holding that:

> [C]onsidering all the relevant circumstances, plaintiffs have not established, and cannot reasonably expect to establish, that the particular conduct of defendants that is challenged in this case was highly offensive and constituted an egregious violation of prevailing social norms. We reach this conclusion from the standpoint of a reasonable person based on defendants' vigorous efforts to avoid intruding on plaintiffs' visual privacy altogether. Activation of the surveillance system was narrowly tailored in place, time, and scope, and was prompted by legitimate business concerns. Plaintiffs were not at risk of being monitored or recorded during regular work hours and were never actually caught on camera or videotape.

Id.

[75] *Id.*

3. *Electronic Monitoring & Eavesdropping*

Private employers will likely retain the ability to video specific places in the workplace as long as the technology does not capture employees conducting tasks. California requires that ALL parties to a telephonic or wire communication consent to its interception and that all parties to a confidential conversation consent to its recording.[76] In fact, the California legislature declared that:

> [A]dvances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. The Legislature by this chapter intends to protect the right of privacy of the people of this state.[77]

An employer need not disclose the contents of any intercepted or recorded conversation to violate California's privacy laws.[78] This would lessen the effectiveness of monitoring employees at their homes or out on the town. However, a California court has held that the communication covered by this section of the penal code does not include covertly taken

---

[76] *See* CAL. PENAL CODE § 632 (West 2010). Stating that a confidential communication:

> [I]ncludes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

Id.

[77] *Id.* § 630.

[78] *See, e.g.*, Coulter v. Bank of Am., 33 Cal. Rptr. 2d 766 (Cal. Ct. App. 1994). Stating that:

> We address briefly the other specific points made by Coulter. First, he suggests that because he never disclosed the tapes to any third party, there was no violation of the Privacy Act. There is no disclosure requirement. Section 632 [of the California Penal Code] prohibits recording a confidential communication without consent of all parties. It says nothing about publishing the communication to a third party.

Id. (internal citation omitted).

video recordings or photographs because such interceptions are not "communications."[79]

4. *Miscellaneous Privacy Protection*

In California, employers cannot punish workers for lawful conduct that occurs during non-working hours and away from the worksite.[80] This is an important distinction from most lifestyle discrimination statutes that merely ban employees from discriminating against employees based on their use of tobacco. California law also states that "[n]o employer shall coerce or influence or attempt to coerce or influence his employees through or by means of threat of discharge or loss of employment to adopt or follow or refrain from adopting or following any particular course or line of political action or political activity."[81]

California requires businesses collecting PII from California residents to post a privacy policy on the homepage stating how they will collect and use PII.[82] California residents may request that companies to which they submitted PII inform them of how their information was disclosed to third

---

[79] *See* People v. Drennan, 101 Cal. Rptr. 2d 584, 589 (Cal. Ct. App. 2000) ("We conclude from the repeated use of words associated with sounds, symbols and hearing that the recordings prohibited by this statute [California Penal Code section 632] are the recordings of the contents of audible or symbol-based communications.").

[80] *See* CAL. LAB. CODE §§ 96(k), 98.6 (West 2010).

[81] *Id.* § 1102 (West 2009).

[82] *See* CAL. BUS. & PROF. CODE § 22575 (West 2009). Stating that the privacy policy must:

> (1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information; (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process; (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service; [and] (4) Identify its effective date.

Id.

parties.[83] Consumers can become aware of their rights in this respect because businesses are required to place a Privacy Policy link on their homepage.[84] Companies that conduct business in California and that collect

---

[83] *See* CAL. CIV. CODE § 1798.83 (West 2009). Stating that the categories of personal information required to be disclosed pursuant to [this provision] are all of the following:

> (i) Name and address; (ii) Electronic mail address; (iii) Age or date of birth; (iv) Names of children; (v) Electronic mail or other addresses of children; (vi) Number of children; (vii) The age or gender of children; (viii) Height; (ix) Weight; (x) Race; (xi) Religion; (xii) Occupation; (xiii) Telephone number; (xiv) Education; (xv) Political party affiliation; (xvi) Medical condition; (xvii) Drugs, therapies, or medical products or equipment used; (xviii) The kind of product the customer purchased, leased, or rented; (xix) Real property purchased, leased, or rented; (xx) The kind of service provided; (xxi) Social security number; (xxii) Bank account number; (xxiii) Credit card number; (xxiv) Debit card number; (xxv) Bank or investment account, debit card, or credit card balance; (xxvi) Payment history; [and] (xxvii) Information pertaining to the customer's creditworthiness, assets, income, or liabilities.

Id.

[84] *Id.* § 1798.83(b)(1)(B) . Stating that a business covered under this section must:

> [A]dd to the home page of its Web site a link either to a page titled "Your Privacy Rights" or add the words "Your Privacy Rights" to the home page's link to the business's privacy policy. If the business elects to add the words "Your Privacy Rights" to the link to the business's privacy policy, the words "Your Privacy Rights" shall be in the same style and size as the link to the business's privacy policy. If the business does not display a link to its privacy policy on the home page of its Web site, or does not have a privacy policy, the words "Your Privacy Rights" shall be written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language. The first page of the link shall describe a customer's rights pursuant to this section and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate. If the business elects to add the words "Your California Privacy Rights" to the home page's link to the business's privacy policy in a manner that complies with this subdivision, and the first page of the link describes a customer's rights pursuant to this section, and provides the designated mailing address, electronic mailing address, as required, or toll-free telephone or facsimile number, as appropriate, the business need not respond to requests that are not received at one of the designated addresses or numbers.

PII must provide "reasonable security" for the information[85] and notify California residents when their PII is compromised.[86] Businesses must also:

> [T]ake all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[87]

California law prohibits the use of RFID technology to read or attempt to read an individual's identification documents.[88] Legislation also states that a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.[89]

F. *Colorado*

1. *Electronic Monitoring & Eavesdropping*

Colorado allows the recording or eavesdropping upon telephonic/ electronic communications and oral conversations as long as one party to the conversation consents to the monitoring.[90] Colorado also criminalizes any conspiracy to wiretap or eavesdrop in a manner inconsistent with the code.[91] However, Colorado law does not "prevent any person from using

---

Id.

[85] *See* CAL. CIV. CODE § 1798.81.5 (West 2010) Defining PII as:

> an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver's license number or California identification card number; (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; [and] (D) Medical information.

Id.

California also protects an individual's Social Security Number (SSN) and Driver's License Number (DLN) in areas such as distribution and retention; *id.* § 1798.85 (discussing SSN); *id.* § 1798.90.1 (discussing DLN).

[86] *See id.* § 1798.82.

[87] *See id.* § 1798.81.

[88] *See id.* § 1798.79.

[89] *See id.*

[90] *See* COLO. REV. STAT. §§ 18-9-303 to 18-9-304 (2010).

[91] *See id.* §§ 18-9-303(1)(f), 18-9-304(1)(d).

wiretapping or eavesdropping devices on his own premises for security or business purposes if reasonable notice of the use of such devices is given to the public." This provision would allow employers to monitor their employees as long as "reasonable notice" is provided.[92] "Reasonable notice" might encompass: (1) receiving notice within a reasonable time prior to the monitoring; (2) reasonably clear and fair terms; or (3) both.

2. *Miscellaneous Privacy Protection*

Colorado law prohibits employers from discriminating against or otherwise coercing employees based on their political affiliations.[93] More specifically, American Jurisprudence stated that these types of prohibitions can be defined as follows:

> The test of whether an employer has violated the statutory prohibition against interference with employees' protected rights does not depend on an employer's motive, courtesy, or gentleness, or on whether the interference, restraint, or coercion succeeded or failed, but on whether an employer engaged in conduct reasonably tending to interfere with the free exercise of employee rights. Stated differently, the issue is not the label placed on the employer's action, but whether the action tends to coerce or not or, considered from the employees' point of view, whether the action had a reasonable tendency to coerce, and a union does not have to demonstrate actual coercion.[94]

Colorado law prohibits termination:

> [O]f any employee due to that employee's engaging in any lawful activity off the premises of the employer during nonworking hours unless such a restriction . . . . relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee . . . [or is] necessary to avoid a conflict of interest with any responsibilities to the employer or the appearance of such a conflict of interest.[95]

---

[92] *See id.* § 18-9-305(1).
[93] *See id.* § 8-2-102.
[94] 48 AM. JUR. 2D *Labor and Labor Relations* § 1336 (2000).
[95] COLO. REV. STAT. § 24-34-402.5 (2010).

Finally, each state governmental entity in Colorado is required to create and post privacy policies that deal with the collection, use, storage and transfer of PII[96] as well as create an e-mail monitoring policy.[97]

G. *Connecticut*

1. *Electronic Monitoring & Eavesdropping*

Like California, Connecticut law requires the consent of all parties before an oral telephonic conversation may be recorded.[98] However, only one party must consent to a recording in cases of wiretapping (or "the intentional overhearing or recording of a telephonic or telegraphic communication or a communication made by cellular radio telephone by a person other than a sender or receiver thereof . . . means of any instrument, device or equipment.").[99] The state code holds that a "person is guilty of eavesdropping when he unlawfully engages in wiretapping or mechanical overhearing of a conversation."[100] State law forbids employers and employees from intentionally overhearing or recording "a conversation or discussion pertaining to employment contract negotiations between the two parties, by means of any instrument, device or equipment, unless such party has the consent of all parties to such conversation or discussion."[101]

In addition, the Code states that a

> [P]erson is guilty of voyeurism when, (1) with malice, such person knowingly photographs, films, videotapes or otherwise records the image of another person (A) without

---

[96] *See id.* § 24-72-502.

[97] *See id.* § 24-72-204.5 (stating that "[o]n or before July 1, 1997, the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system shall adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted.").

[98] *See* CONN. GEN. STAT. § 52-570d (2010). Stating that any recording must be:

> (1) preceded by consent of all parties to the communication and such prior consent either is obtained in writing or is part of, and obtained at the start of, the recording, or (2) is preceded by verbal notification which is recorded at the beginning and is part of the communication by the recording party, or (3) is accompanied by an automatic tone warning device which automatically produces a distinct signal that is repeated at intervals of approximately fifteen seconds during the communication while such instrument, device or equipment is in use.

Id.

[99] *Id.* § 53a-187.

[100] *Id.* § 53a-189.

[101] *Id.* § 31-48b(d).

> the knowledge and consent of such other person, (B) while such other person is not in plain view, and (C) under circumstances where such other person has a reasonable expectation of privacy . . . .[102]

In addition, Connecticut state law forbids employers to operate

> [A]ny electronic surveillance device or system, including but not limited to the recording of sound or voice or a closed circuit television system . . . for the purpose of recording or monitoring the activities of his employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as restrooms, locker rooms or lounges.[103]

The first two violations of this provision can lead to fines with additional violations leading to up to thirty days imprisonment.[104]

2. *Miscellaneous Privacy Protection*

Connecticut is one of only two states that require employers to notify their employees before implementing electronic monitoring.[105] This groundbreaking statute reads:

> [E]ach employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur. Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice.[106]

This notice requirement does not apply when "an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct."[107] These provisions do not apply when the employee is under a criminal investigation.[108] Violations of this provision lead to investigations by the

---

[102] *Id.* § 53a-189a.
[103] *Id.* § 31-48b(b).
[104] *See id.* § 31-48b(c).
[105] *See id.* § 31-48d.
[106] *Id.* § 31-48d(b)(1).
[107] *Id.* § 31-48d(2)(A)(B).
[108] *See id.* § 31-48d(d).

Connecticut Labor Commissioner; after such investigations, the Commissioner may levy fines which increase as the number of violations increases.[109]

Connecticut has enacted a lifestyle discrimination statute that prohibits employers from disciplining or discharging employees:

> [O]n account of the exercise by such employee of rights guaranteed by the first amendment to the United States Constitution or section 3, 4 or 14 of article first of the Constitution of the state,[110] provided such activity does not substantially or materially interfere with the employee's bona fide job performance or the working relationship between the employee and the employer.[111]

Connecticut law also prohibits employers from conditioning employment upon or in any way discriminating against an employee because of lawful use of tobacco products outside of the workplace.[112] Finally, businesses must create and post a privacy policy if they collect Social Security Numbers in the course of business.[113] Finally, Connecticut requires an employee's consent before an employer may release a personnel file to a third party.[114]

H. *Delaware*

1. *Electronic Monitoring & Eavesdropping*

Delaware law states that no individual shall "[i]ntentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any wire, oral or electronic communication."[115] It is lawful, however, for "a person to intercept a wire, oral or electronic communication

---

[109] *See id.* § 31-48d(c).

[110] The First Amendment to the United States Constitution protects all United States citizens in their rights to freedom: (1) of speech, (2) of religion (allowing for free exercise and prohibiting the establishment of religion), (3) of the press, (4) of assembly, and (5) to petition the government for the redress of grievances. *See* U.S. CONST. amend. I. These sections mentioned in this statute protect all Connecticut citizens in their rights to religious profession and worship, freedom of speech and to petition the government for the redress of their grievances. *See* CONN. CONST. art. I, §§ 3, 4, 14.

[111] CONN. GEN. STAT. § 31-51q (2010).

[112] *See id.* § 31-40s (stating that any "nonprofit organization or corporation whose primary purpose is to discourage use of tobacco products by the general public shall be exempt from the provisions of this section.").

[113] *See id.* § 42-471(b).

[114] *See id.* § 31-128f.

[115] *See* DEL. CODE ANN. tit. 11, § 2402(a)(1) (2010).

where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception."[116] The law seemingly conflicts with Delaware's privacy law which states that:

> A person is guilty of a violation of privacy when . . . the person:
>
> 1. Trespasses on property intending to subject anyone to eavesdropping or other surveillance in a private place; or
> 2. Installs in any private place, without consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place; or
> 3. Installs or uses outside a private place any device for hearing, recording, amplifying or broadcasting sounds originating in that place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy there; or
> 4. Intercepts without the consent of all parties thereto a message by telephone, telegraph, letter or other means of communicating privately, including private conversation.[117]

This conflict made its way to the Delaware courts where one opinion held that Delaware law regarding interception was intended to mirror federal law where only one party to a conversation need consent.[118] Also, the Delaware Electronic Surveillance and Interception of Communications Statute[119] is much more recent than the Delaware Privacy Statute.[120] It is reasonable to assume that the state legislature knew of the consent provisions on the Privacy Act when it allowed for only one person to consent to wiretapping. Finally, the privacy statute prohibits anyone from making "tape records, photographs, films, videotapes or otherwise [reproducing] the image of another person" who disrobes in private places where such person has a reasonable expectation of privacy.[121] By its terms, this provision would likely not prohibit an employer placing a video camera in an employee break room where disrobing—hopefully—is uncommon. It would likely prohibit cameras in restrooms, employee locker rooms and in offices where employees may change clothes.

---

[116] *Id.* § 2402(c)(4).
[117] *Id.* § 1335(a)(1)–(4).
[118] United States v. Vespe, 389 F. Supp. 1359, 1372 (D. Del. 1975).
[119] *See* 72 Del. Laws 391 (1999).
[120] Enacted in 1953. *See* 58 Del. Laws 497 (1999); 67 Del. Laws 130 (1999); 70 Del. Laws 186 (1953); *see also* CAN WE TAPE?, *supra* note 41, at Del. (stating that the "wiretapping law is much more recent, and at least one federal court has held that, even under the privacy law, an individual can record his own conversations.").
[121] DEL. CODE ANN. tit. 11, § 1335(a)(6) (2010).

2. *Miscellaneous Privacy Protection*

Delaware is also on the front lines in the battle of employee notice of electronic monitoring. Delaware's Labor Code states that employers may not:

> [M]onitor or otherwise intercept any telephone conversation or transmission, electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer either:
>
> 1. Provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer-provided e-mail or Internet access services; or
> 2. Has first given a [one time] notice to the employee of such monitoring or intercepting activity or policies. The notice required by this paragraph shall be in writing, in an electronic record, or in another electronic form and acknowledged by the employee either in writing or electronically.[122]

Problematically, the law only allows for a $100 fine per violation.[123] These fines could add up, however, due to the statute's daily notice requirement. And, employees are allowed to pursue other remedies—including an invasion of privacy tort lawsuit.[124] Finally, state agencies that maintain a website are required to develop a privacy policy dictating how they deal with personal information.[125]

I. *Florida*

1. *Constitutional Privacy Protection*

Florida's Constitution provides its citizens with a right to privacy.[126] Article I, section 12 states that "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and

---

[122] *Id.* at tit. 19, § 705(b)(1)–(2). "The provisions of this section shall not apply to processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or Internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection." *Id.* § 705(e).

[123] *Id.* § 705(c).

[124] *Id.* § 705(d).

[125] *Id.* at tit. 29, § 9018C.

[126] FLA. CONST. art. I, §§ 12, 23.

seizures, and against the unreasonable interception of private communications by any means, shall not be violated."[127] The "interception of private communications" clause is an addition to the language that was otherwise derived from the Fourth Amendment of the United States Constitution.[128] And, like the Fourth Amendment, Florida's clause only applies to invasions of privacy by state actors.[129] Article I, § 23 of the Florida Constitution states that "[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[130] By its own terms, § 23 is limited to state action that violates an individual's privacy. Additionally, Florida's privacy provision "has not been given the power that was intended when it was adopted in 1980."[131]

2. *Electronic Monitoring & Eavesdropping*

Florida is one of the few states that requires that all parties consent to any recording of an oral, wire, or electronic communication.[132] "Under the [Florida Security of Communications Act] statute, consent is not required for the taping of a non-electronic communication uttered by a person who does not have a reasonable expectation of privacy in that

---

[127] *Id.* § 12.

[128] *Id.*; U.S. CONST. amend. IV.

[129] *See, e.g.*, State v. Abislaiman, 437 So. 2d 181, 183 n.2 (Fla. Dist. Ct. App. 1983) (discussing, among other things, Article 1, Section 12 and stating that "[s]ince it was not made an issue in the trial court, the state has conceded for purposes of this appeal that Officer Nieto's activities at all relevant times constituted state action."); s*ee also* State v. Tsavaris, 382 So. 2d 56, 66 (Fla. Dist. Ct. App. 1980) (questioned by a later case on other grounds). Stating that:

> Although presumably Article I, Section 12 [of the Florida Constitution], applies only to state action as distinguished from private action, the argument could be made that Dr. Feegel's action in recording his first telephone conversation with Dr. Tsavaris was state action in view of the fact that Dr. Feegel held the office of medical examiner pursuant to Florida law and was acting in that capacity at the time. In our view, participant recording of a conversation is not an interception of a private communication. Therefore, Article I, Section 12, is not applicable.

Id.

[130] FLA. CONST. art. I, § 23.

[131] Deborah Lynn Stewart, Note and Comment, City of North Miami v. Kurtz–*Is It Curtains for Privacy In Florida?*, 20 NOVA L. REV. 1393, 1399 (Spring 1996) (citing other sources and stating that "[i]t has been observed that 'all too often privacy plays second banana to competing interests,' even though the purpose of this provision was to provide more protection").

[132] FLA. STAT. § 934.03(2)(d) (2010).

communication."[133] This all-parties consent provision was added to the Florida law in 1974 via an amendment.[134] This amendment:

> [W]as a policy decision by the Florida legislature to allow each party to a conversation to have an expectation of privacy from interception by another party to the conversation . . . . Hence, the Florida act evinces a greater concern for the protection of one's privacy interests in a conversation than does the federal act.[135]

However, Florida courts have held that businesses are allowed to record telephone calls without the consent of all parties.[136] The court held that the Florida Security of Communications law was intended to resemble the Federal Wiretap Act,[137] which only requires one party to a conversation to consent when such recording is made in the ordinary course of business.[138] At the end of the day, Florida employers are wise to consult counsel before wading through these provisions.

---

[133] CAN WE TAPE?, *supra* note 41, at Fla. (citing the definition of "oral communication" in FLA. STAT. § 934.02 (2010)).

[134] *Tsavaris*, 394 So. 2d at 422 n.5.

[135] *Id.* at 422 (citing Shevin v. Sunbeam Television Corp., 351 So. 2d 723, 726–27 (Fla. 1977)).

[136] Royal Health Care Servs., Inc. v. Jefferson-Pilot Life Ins. Co., 924 F.2d 215, 219 (11th Cir. 1991). Holding that:

> Florida does indeed have a two-party consent rule. But we disagree with Royal Health's contention that all federal case law dealing with the Federal Wiretap Act is inapposite. The Historical Note that follows the legislative findings section of the Act indicates that, with one exception the [Florida] state law follows closely the federal act.

Id. (internal quotations omitted).

[137] *Id.* The Federal Wire Act reads, in the relevant part:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d) (2010).

[138] 18 U.S.C. § 2511(2)(d).

J. *Georgia*

1. *Electronic Monitoring & Eavesdropping*

When it comes to the interception of communications, Georgia law is a bit complicated. The law requires the consent of both parties before any private conversation may be overheard, transmitted or recorded.[139] For interceptions to be illegal, they must be made in a clandestine manner and must originate in a private place.[140] Georgia law also prohibits any person from "intentionally and secretly [intercepting] by the use of any device, instrument, or apparatus the contents of a message sent by telephone, telegraph, letter, or by any other means of private communication."[141] However, a specific exception exists which allows "a person [to intercept] a wire, oral, or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[142] Therefore, employers can record their employees as long as they are a party to the communication but not when the employer is not a party to a private conversation made in a private place.

Finally, it is unlawful for anyone "through the use of any device . . . to observe, photograph, or record the activities of another which occur in any private place and out of public view" without the consent of all parties involved.[143] As stated earlier, there are few places in the workplace that are considered truly private. This state law would not apply to surveillance in public areas of the workplace.

K. *Hawaii*

1. *Constitutional Privacy Protection*

Hawaii's Constitution provides for a right to privacy. Article I, section 6 states that "[t]he right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."[144] Section 7 of article I states that:

> The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and *invasions of privacy* shall not be violated; and

[139] GA. CODE ANN. § 16-11-62 (2010).
[140] *Id.* § 16-11-62(1).
[141] *Id.* § 16-11-62(4).
[142] *Id.* § 16-11-66(a).
[143] *Id.* § 16-11-62(2).
[144] HAW. CONST. art I, § 6.

> no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted.[145]

These sections have been held to apply only to invasions of privacy committed by state actors.[146]

2. *Electronic Monitoring & Eavesdropping*

In Hawaii, an interception of an oral, wire or electronic communication is valid as long as one party to the communication intercepts or as long as one party to the communication consents to the interception.[147] Such interceptions are valid as long as no criminal or tortious intent exists.[148] Hawaii law does not allow people to place recording devices in private places.[149] Any installation or use in a private place and without consent of any device capable of observing, recording, amplifying, or broadcasting a person in a state of undress constitutes a violation of privacy in the first degree.[150] More applicable to the employment environment, a violation of privacy in the second degree occurs when a person:

> (d) Installs or uses, or both, in any private place, without consent of the person or persons entitled to

---

[145] *Id.* § 7 (emphasis added).

[146] *See, e.g.*, State v. Mallan, 950 P.2d 178, 184 (Haw. 1998) (stating that article I, § 6 of the Hawaii Constitution should be interpreted under the rational basis to strict scrutiny tests adopted by the United States Supreme Court to determine the invasiveness of state action). The dissent in the same opinion stated that "article I, section 6 of the Hawaii Constitution . . . which has given an express and expansive local home to the proposition . . . that 'the right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest.'" *Id.* at 193 (Levinson, J., dissenting). The same holds true for article I, § 7; for example:

> The right-to-privacy provisions in article I, section 6 and article I, section 7 [of the Hawaii Constitution] are distinct. As the final interpreter of the Hawaii Constitution, the Hawaii Supreme Court has so held . . . . This history also makes it clear that the right to privacy protected by article I, section 7 is not in the nature of a fundamental right. Rather, its application is limited to criminal cases and is to be construed in light of the language [of the United States Supreme Court] regarding reasonable expectations of privacy.

State v. Okuba, 651 P.2d 494, 500 (Haw. Ct. App. 1982).

[147] HAW. REV. STAT. § 803-42(b)(3)(A) (2010).

[148] *Id.*

[149] *Id.* § 711-1110.9.

[150] *Id.* (stating that the consent must come from the person who holds the right to privacy in the private place).

> privacy therein, any means or device for observing, recording, amplifying, or broadcasting sounds or events in that place, including another person in a stage of undress or sexual activity;
>
> (e) Installs or uses outside a private place any device for hearing, recording, amplifying, or broadcasting sounds originating in that place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy therein; [or, for purposes of this discussion] . . . ;
>
> (g) Intercepts, without the consent of the sender or receiver, a message or photographic image by telephone, telegraph, letter, electronic transmission, or other means of communicating privately.[151]

For obvious reasons, it is more likely that an employer would find itself in hot water for a violation of privacy in the second degree. Violations in the first degree require employers to surveil in areas that they know are private—such as locker rooms, restrooms, etc.—where employees are likely to be in any "stage of undress." Second degree privacy invasions might apply to surveillance inside or just outside of employee offices or communications such as e-mails that employees consider private.

L. *Idaho*

1. *Electronic Monitoring & Eavesdropping*

In Idaho, "[a]lthough legislation criminalizes the interception and disclosure of wire, [electronic,] or oral communications, it specifically allows interception when one of the parties [to the communication] has given prior consent."[152] Idaho law states that a crime is committed with a willful interception, an attempt to intercept, or an arrangement to intercept or attempt to intercept a communication without the necessary consent covered under the statute.[153]

---

[151] *Id.* § 711-1111(1)(d), (e), (g).

[152] CAN WE TAPE?, *supra* note 41, at Idaho (citing IDAHO CODE ANN. § 18-6702 (2010)).

[153] IDAHO CODE ANN. §18-6702(1) (2010).

M. *Illinois*

1. *Constitutional Privacy Protection*

The Illinois Constitution protects an Illinois citizen's right to privacy.[154] Article I, § 6 states, in pertinent part, that "[t]he people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, *invasions of privacy or interceptions of communications by eavesdropping devices or other means*."[155] Article I, § 12, of the state constitution declares that "[e]very person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, *privacy*, property or reputation. He shall obtain justice by law, freely, completely, and promptly."[156] Section 6 only applies to invasions of privacy and interceptions of communications caused by state action.[157] Section 12, on the other hand, has been held to apply to private entities as well as state action.[158] The Illinois Supreme Court held that:

> Consistent with this court's [prior holding] we recognize that section 12 of the Illinois Constitution, unlike section 6, does not require state action before its protections are activated. However, the precise nature and scope of the privacy interest set forth in section 12 has not been the subject of much case law in this state.[159]

The court continued on to state that "[w]e do not, however, create a broad-based remedy for perceived violations of a person's privacy interests by private parties. Instead, we focus narrowly on the constitutional source of the privacy interest that can be deemed a part of the public policy of this state."[160] In other words, § 12 does not create a private right of action for invasions of privacy; rather, the section "simply expresses a public policy philosophy with which Illinois statutes must comply."[161]

---

[154] ILL. CONST. art I, §§ 6, 12.
[155] *Id.* § 6 (emphasis added).
[156] *Id.* § 12 (emphasis added).
[157] Best v. Taylor Mach. Works, 689 N.E.2d 1057, 1097 (Ill. 1997) (citing precedent and stating that "[t]his court has stated that governmental conduct or 'state action' must be present before a citizen claiming a violation of the privacy right referenced in section 6 of the Illinois Bill of Rights may obtain relief.").
[158] *Id.*
[159] *Id.*
[160] *Id.* at 1100 n.13.
[161] Belleville v. Cottrell, Inc., No. 09-CV-962-JPG, 2010 WL 1251442, at *4 (S.D. Ill. Mar. 24, 2010) (construing *Best*, 689 N.E.2d 1057).

2. *Electronic Monitoring & Eavesdropping*

Furthermore, Illinois law requires the consent of all parties to authorize any intentional and knowing use of "an eavesdropping device for the purpose of hearing or recording all or any part of *any conversation*" or the interception, retention or transcription of an electronic communication.[162] Illinois law states that it is not unlawful for "a provider of wire or electronic communication services, their agents, employees, contractors, or venders to . . . possess an eavesdropping device within the normal course of their business for purposes not contrary to this Article."[163] The statute also provides an affirmative defense for individuals who illegally intercept communications as long as such individuals do not disclose the contents of the communication they obtain.[164] "An eavesdropping device is any device capable of being used to hear or record oral conversation or intercept, retain, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means . . . ."[165] This definition is important because it criminalizes the interception of an in-person communication as well as an electronic communication. Also, Illinois law states that "[i]t is unlawful for any person to knowingly make a video record or transmit live video of another person without that person's consent in a restroom, tanning bed, tanning salon, locker room, changing room, or hotel bedroom."[166] Although sound recording is not covered under this section, employers would be prohibited from placing video cameras in private places on the worksite.[167]

3. *Miscellaneous Privacy Protection*

Illinois law also contains the Right to Privacy in the Workplace Act (RPWA). The RPWA states that "it shall be unlawful for an employer to

---

[162] 720 ILL. COMP. STAT. 5/14-2(a)(1) (2010) (emphasis added).
[163] *Id.* at 5/14-2(c).
[164] *Id.* at 5/14-2(b)(4).
[165] *Id.* at 5/14-1(a). Stating also that:

> [T]he term electronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, where the sending and receiving parties intend the electronic communication to be private and the interception, recording, or transcription of the electronic communication is accomplished by a device in a surreptitious manner contrary to the provisions of this Article.

Id. at 5/14-1(e).
[166] *Id.* at 5/26-4(a).
[167] *Id.* at 5/26-4(c).

refuse to hire or to discharge any individual, or otherwise disadvantage any individual, with respect to compensation, terms, conditions or privileges of employment because the individual uses lawful products off the premises of the employer during nonworking hours."[168] The State of Illinois has also created an Internet Privacy Task Force—a seventeen-member body tasked to:

> Explore the technical and procedural changes that are needed in the State's computing environment to ensure that visits to State Web sites remain private. The Task Force shall identify the threats to privacy from browsers, search engines, Web servers, Internet service providers, and State agencies and make recommendations as needed. If needed, the Task Force shall devise procedures for creating or installing computer programs on State host computers that will disable cookies and other invasive programs.[169]

Illinois state agencies are not allowed to "use permanent cookies or any other invasive tracking programs that monitor and track Web site viewing habits."[170] However, state agency Web sites "may use transactional cookies that facilitate business transactions."[171] Each state agency in Illinois is required to produce an "identity-protection policy" that deals with the use and handling of social security numbers.[172]

N. *Indiana*

1. *Electronic Monitoring & Eavesdropping*

Before a third party may intercept an electronic communication, Indiana law requires the consent of either the sender or receiver.[173] The sender or receiver of the communication itself may record without the

---

[168] 820 ILL. COMP. STAT. 55/5(a) (2010).
[169] 5 ILL. COMP. STAT. 177/15(b) (2010).
[170] *Id.* at 177/10(a). The statute states:

> Permanent cookies used by State agency Web sites may be exempt from the prohibition in subsection (a) if they meet the following criteria: (1) The use of permanent cookies adds value to the user otherwise not available; (2) The permanent cookies are not used to monitor and track web site viewing habits unless all types of information collected and the State's use of that information add user value and are disclosed through a comprehensive online privacy statement.

Id. at 177/10(b)(1)–(2).
[171] *Id.* at 177/10(a).
[172] *Id.* at 179/37.
[173] IND. CODE § 35-33.5-1-5 (2010).

consent of the other party.[174] An "[e]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, oral communication, digital information, or intelligence of any nature transmitted in whole or in part by a wire, a radio, or an electromagnetic, a photoelectronic, or a photo-optical system."[175]

2. *Miscellaneous Privacy Protection*

Employers in Indiana may not "require . . . an employee or prospective employee to refrain from using; or discriminate against an employee . . . based on the employee's use of; tobacco products outside the course of the employee's or prospective employee's employment."[176] Interestingly, the state code allows employers to use financial incentives which are "intended to reduce tobacco use" as long as such benefits are "related to employee health benefits provided by the employer."[177]

O. *Iowa*

1. *Electronic Monitoring & Eavesdropping*

Iowa law has an interesting twist on the one-party consent provisions of other states. The state code allows the sender or the receiver of a communication (or someone present and participating in or listening to a communication) to consent to its interception.[178] Otherwise:

> Any person, having no right or authority to do so, who taps into or connects a listening or recording device to any telephone or other communication wire, or who by any electronic or mechanical means listens to, records, or otherwise intercepts a conversation or communication of any kind, commits a serious misdemeanor . . . .[179]

Another provision of Iowa law states that one party to a communication may consent to the willful interception or a wire, oral, or electronic communication.[180] This potential conflict between statutory provisions has reared its head in at least one case.[181] An employee of the Franklin County Clerk's Office—distraught at her relationships between her and her co-workers—secretly tape-recorded conversations from her desk throughout

---

[174] *Id.*
[175] *Id.* § 35-33.5-1-3.5.
[176] *Id.* § 22-5-4-1.
[177] *Id.*
[178] IOWA CODE § 727.8 (2010).
[179] *Id.*
[180] *Id.* § 808B.2 (2010).
[181] *See, e.g.*, State v. Philpott, 702 N.W.2d 500 (Iowa 2005).

the work day.[182] The employee was charged under Iowa Code § 727.8 rather than § 808B.2.[183] The district court spent a large part of the opinion discussing the interplay between the two interception statutes.[184]

2. *Miscellaneous Privacy Protection*

The Iowa Fair Information Practices Act requires state agencies to create information policies that detail, among other things:

1. The nature and extent of the personally identifiable information collected by the agency, the legal authority for the collection of that information, and a description of the means of storage.
2. The procedures by which the agency shall notify persons supplying information requested by the agency of the use that will be made of the information, which persons outside of the agency might routinely be provided this information, which parts of the information requested are required and which are optional and the consequences of failing to provide the information requested.
3. Whether a data processing system matches, collates, or permits the comparison of personally identifiable information in one record system with personally identifiable information in another record system.[185]

P. *Kansas*

1. *Electronic Monitoring & Eavesdropping*

Kansas' state code contains a section titled "Breach of Privacy."[186] Under Kansas law, "[i]ntercepting, without the consent of the sender or receiver, a message by telephone, telegraph, letter or other means of private communication" is a Class A misdemeanor.[187] This provision places Kansas with the other states that allow interceptions of communications as

---

[182] *Id.* at 502.
[183] *Id.; see also* State v. Philpott, No. 04-0060, 2005 WL 156824, at *1 (Iowa Ct. App. 2005).
[184] *Philpott*, 2005 WL 156824, at *2; *see also* State v. Fox, 493 N.W.2d 829, 831 (Iowa 1992) (discussing the interplay between the two statutes).
[185] IOWA CODE § 22.11(1)(a), (f), (g) (2010).
[186] *See* KAN. STAT. ANN. § 21-4002 (2009).
[187] *Id.* § 21-4002(1).

long as one party to the communication consents. The state also prohibits eavesdropping which is defined as:

> 1. [E]ntering into a private place with intent to listen surreptitiously to private conversations or to observe the personal conduct of any other person or persons therein;
> 2. [I]nstalling or using outside a private place any device for hearing, recording, amplifying or broadcasting sounds originating in such place, which sounds would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy therein;
> 3. [I]nstalling or using any device or equipment for the interception of any telephone, telegraph or other wire communication without the consent of the person in possession or control of the facilities for such wire communication; or
> 4. [I]nstalling or using a concealed camcorder, motion picture camera or photographic camera of any type, to secretly videotape, film, photograph or record by electronic means, another, identifiable person under or through the clothing being worn by that other person or another, identifiable person who is nude or in a state of undress, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, with the intent to invade the privacy of that other person, under circumstances in which the other person has a reasonable expectation of privacy.[188]

A private place under the law is defined as "a place where one may reasonably expect to be safe from uninvited intrusion or surveillance, but does not include a place to which the public has lawful access."[189] There is the potential for an eavesdropping employer to be charged under both the Breach of Privacy Statute and the eavesdropping statute. In addition, the Kansas Supreme Court "has interpreted the eavesdropping and privacy statutes to allow one-party consent for taping of conversations and in interpreting both statutes has held that as long as one party consents to the conversation, the other party loses his right to challenge the eavesdropping in court."[190] Finally, the Kansas eavesdropping statute would prevent

---

[188] *See id.* § 21-4001.

[189] *Id.* § 21-4001(b).

[190] *See* CAN WE TAPE? *supra* note 41, at Kan. (citing State v. Roudybush, 686 P.2d 100, 109 (Kan. 1984)).

employers from secretly recording employees in private places, such as locker rooms or restrooms and perhaps even employee offices.

Q. *Kentucky*

1. *Electronic Monitoring & Eavesdropping*

In Kentucky, it is a Class D felony when a person "intentionally uses any device to eavesdrop, whether or not he is present at the time."[191] The state code states that to eavesdrop "means to overhear, record, amplify or transmit any part of a wire or oral communication of others without the consent of at least one (1) party thereto by means of any electronic, mechanical or other device."[192] It does not matter when the interception device is placed as long as it is placed "with the knowledge that it is to be used for eavesdropping."[193] A person is not guilty of eavesdropping if she "[i]nadvertently overhears the communication through a regularly installed telephone party line or on a telephone extension but does not divulge it."[194]

2. *Miscellaneous Privacy Protection*

It is unlawful in Kentucky:

> To fail or refuse to hire, or to discharge any individual, or otherwise to discriminate against an individual with respect to compensation, terms, conditions, or privileges of employment . . . because the individual is a smoker or nonsmoker, as long as the person complies with any workplace policy concerning smoking.[195]

In addition, employers cannot "require as a condition of employment that any employee or applicant for employment abstain from smoking or using tobacco products outside the course of employment, as long as the person complies with any workplace policy concerning smoking."[196]

---

[191] KY. REV. STAT. ANN. § 526.020(1) (West 2009).
[192] *Id.* § 526.010.
[193] *Id.* § 526.030(1).
[194] *Id.* § 526.070(1).
[195] *Id.* § 344.040(1).
[196] *Id.* § 344.040(3).

R. *Louisiana*

1. *Constitutional Privacy Protection*

Article I, § 5 of the Louisiana Constitution is entitled "Right to Privacy."[197] This provision states:

> Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or *invasions of privacy.* No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.[198]

As with other state constitutional privacy protections, Louisiana's Article I, § 5 only applies to state action.[199] The Louisiana Supreme Court "concluded that an individual is entitled to recover money damages for any injury he has suffered as a result of a *state agent's* violation of Article I, § 5 of the 1974 Louisiana Constitution."[200]

2. *Electronic Monitoring & Eavesdropping*

Only one party must consent to the interception of a wire, oral or electronic communication in Louisiana.[201] This is not true if the intercepting party has a criminal or tortious intent or intercepts the communication "for the purpose of committing any other injurious act."[202] Louisiana has adopted a lifestyle discrimination statute that protects employees who smoke tobacco while off-duty.[203] This statute states that employees who comply with "applicable law and any adopted workplace policy regulating smoking" are protected.[204] In fact:

> [I]t shall be unlawful for an employer: (1) To discriminate against the individual with respect to discharge, compensation, promotion, any personnel action or other condition, or privilege of employment because the

[197] LA. CONST. art. I, § 5.
[198] *Id.* (emphasis added).
[199] *See* Moresi v. State, 567 So. 2d 1081, 1093 (La. 1990).
[200] *Id.* (emphasis added).
[201] *See* LA. REV. STAT. ANN. § 15:1303 (2010).
[202] *Id.* § 15:1303(c)(4).
[203] *See id.* § 23:966.
[204] *Id.* § 23:966(A).

> individual is a smoker or nonsmoker [and] (2) To require, as a condition of employment, that the individual abstain from smoking or otherwise using tobacco products outside the course of employment.[205]

Louisiana law also criminalizes video voyeurism as follows:

> 1. The use of any camera, videotape, photo-optical, photo-electric, or any other image recording device for the purpose of observing, viewing, photographing, filming, or videotaping a person where that person has not consented to the observing, viewing, photographing, filming, or videotaping and it is for a lewd or lascivious purpose; or
> 2. The transfer of an image obtained by activity described in Paragraph (1) of this Subsection by live or recorded telephone message, electronic mail, the Internet, or a commercial online service.[206]

3. *Especially Relevant Case Law*

A Louisiana court recently dealt with video monitoring of employees. In one of the state's most prominent monitoring cases, a security officer working for a private employer (Wal-Mart) allegedly violated the privacy rights of forty-five employees when he installed a video camera in a unisex restroom.[207] This was done without the permission of Wal-Mart management.[208] Suspecting theft by the night crew, the security officer placed a remote-controlled camera in the ceiling tile of the employee restroom.[209] The idea was to record action at the doorway to discover whether employees were entering the restroom with merchandise.[210] The

---

[205] *Id.* § 23:966(A)(1)–(2).

[206] *Id.* § 14:283(A)(1)–(2).

[207] *See* Meche v. Wal-Mart Stores, Inc., 692 So. 2d 544, 545 (La. Ct. App. 1997).

[208] See *id.* at 546–47.

[209] *See id.* at 546. Stating that the security officer:

> [H]ad reason to believe that a member of the night receiving crew was stealing merchandise from the store by taking it to either the break room or the employee restroom, removing the item from its packaging, and concealing the pilfered item under his/her clothing. Feeling the restroom was the most likely place of occurrence of the suspected offenses, [the officer] decided to [conceal] a closed circuit television camera in the ceiling of the employee restroom in an attempt to apprehend the suspect.

Id.

[210] *Id.*

camera was discovered by a female employee who was using the restroom as it slipped through the tile into plain view.[211] In the end, the receiver was never connected to the recording device and no footage was recorded.[212] The security officer was terminated and Wal-Mart concluded an internal investigation; the forty-five employees who claimed that they had used the restroom during the time that the camera was installed were unsatisfied with the process and filed a lawsuit.[213] The court sided with Wal-Mart holding that, at most, the company committed an attempted invasion of privacy—an action that is not a recognized tort.[214] The employees' ECPA claim was also dismissed considering that:

> Not only was there no interception of any electronic transmission, but the [ECPA] limits recovery to 'any persons whose wire, aural or electronic communication is intercepted, disclosed, or intentionally used . . . the plaintiffs neither initiated nor engaged in any communication of any sort. The conduct, of which they complain simply, does not fit the conduct proscribed by the statute."[215]

For some reason, the plaintiffs in the case brought suit under the Federal ECPA rather than Louisiana's wiretapping statute. The same result may have resulted or the court may have determined that the employer (through its agent) had tortious intent (invasion of privacy) in making the interception.

4. *Miscellaneous Privacy Protection*

Louisiana has a strong employee protection law when it comes to an individual's political activities. The state code dictates that:

> [N]o employer having regularly in his employ twenty or more employees shall make, adopt, or enforce any rule, regulation, or policy forbidding or preventing any of his employees from engaging or participating in politics, or from becoming a candidate for public office. No such

---

[211] *See id.*

[212] *See id.* (stating that the security officer admitted he had "placed the camera in the restroom ceiling and explained his motive was to attempt to catch a thief. He maintained that the receiver had never been connected to either a monitor or a VCR and that neither he nor anyone else had viewed or taped anyone in the restroom.").

[213] See *id.* at 547.

[214] *See id.* at 547 (holding that "[a]t best, we consider the facts herein to have established an attempted invasion of privacy. However, since we know of no such tort, we find we have no choice but to find there was no clear error committed by the trial judge [in ruling for Wal-Mart].").

[215] *Id.*

> employer shall adopt or enforce any rule, regulation, or policy which will control, direct, or tend to control or direct the political activities or affiliations of his employees, nor coerce or influence, or attempt to coerce or influence any of his employees by means of threats of discharge or of loss of employment in case such employees should support or become affiliated with any particular political faction or organization, or participate in political activities of any nature or character.[216]

Violations of this statute may result in a fine or imprisonment, or both.[217] Employees injured in this manner may also sue to recover in a civil action against their employer.[218]

S. *Maine*

1. *Electronic Monitoring & Eavesdropping*

Maine allows one party to an oral or wire communication the authority to make an interception of such communication.[219] State law defines the term "intercept" to mean:

> [T]o hear, record or aid another to hear or record the contents of any wire or oral communication through the use of any intercepting device by any person other than: (A) The sender or receiver of that communication; (B) A person within the range of normal unaided hearing or subnormal hearing corrected to not better than normal; or (C) A person given prior authority by the sender or receiver.[220]

In fact, most individuals in Maine are prohibited from possessing or selling interception-capable devices.[221] Maine law bans hidden cameras and other recording devices inside "private places."[222] The same statute bans listening devices outside of private places which are able to record sounds that would not otherwise be audible.[223] The term "private place"

---

[216] LA. REV. STAT. ANN. § 23:961 (2010).
[217] *Id.*
[218] *Id.*
[219] ME. REV. STAT. ANN. tit. 15, § 710 (2010).
[220] *Id.* § 709(4).
[221] *See id.* § 709(5)–(6).
[222] *Id.* at tit. 17-A, § 511(1)(B) (stating that a person is guilty of invasion of privacy if he or she "[i]nstalls or uses in a private place without the consent of the person or persons entitled to privacy in that place, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place.").
[223] *See id.* § 511(1)(C).

means "a place where one may reasonably expect to be safe from surveillance, including, but not limited to, changing or dressing rooms, bathrooms and similar places."[224]

2. *Miscellaneous Privacy Protection*

In accordance with many other states, Maine law prohibits employers from discriminating against their employees based on the latter's use of tobacco. The law states that:

> An employer or an agent of an employer may not require, as a condition of employment, that any employee or prospective employee refrain from using tobacco products outside the course of that employment or otherwise discriminate against any person with respect to the person's compensation, terms, conditions or privileges of employment for using tobacco products outside the course of employment as long as the employee complies with any workplace policy concerning use of tobacco.[225]

T. *Maryland*

1. *Electronic Monitoring & Eavesdropping*

Maryland is one of the few states that requires all parties to consent to the interception of an oral, electronic, or wire communication.[226] More specifically, Maryland law states that it is lawful:

> [F]or a person to intercept a wire, oral, or electronic communication where the person is a party to the communication and where all of the parties to the communication have given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this State.[227]

This specificity is rather unique in the fact that, even if all parties consent to the interception, at least one of the consenting parties must also be a party to the conversation. This would prevent an employer from monitoring an employee's conversation with a third party unrelated to the

---

[224] *Id.* § 511(2).
[225] *Id.* at tit. 26, § 597.
[226] *See* MD. CODE ANN., CTS. & JUD. PROC. § 10-402(c)(3) (LexisNexis 2010).
[227] *Id.*

employer. Violations of this statute are felonies punishable by imprisonment of up to five years, a $10,000 fine or both.[228]

In addition, it is unlawful in Maryland to use a hidden recording device or an individual's eyes to peer into a "private place" without the consent of the individual being viewed.[229] "Private place" in section 93-901 of the Maryland Criminal Code is confined by its definition as a dressing room or a rest room in a retail store.[230] The code authorizes a civil action against the perpetrator of the surveillance and also states that it is "not a defense to a prosecution under this section that the defendant owns the premises where the private place is located."[231] Maryland law also criminalizes visual surveillance with prurient (sexual) intent.[232] This is not as likely (hopefully) to arise in the context of employee monitoring. Under this section of the Criminal Code a "private place" is defined more loosely as "a room in which a person can reasonably be expected to fully or partially disrobe and has a reasonable expectation of privacy."[233] An expectation exists allowing surveillance without prurient intent by a person who conducts such visual surveillance to protect property.[234]

2. *Miscellaneous Privacy Protection*

Maryland law also prohibits individuals and businesses from requiring the use of SSNs or transmitting SSNs over the Internet (unless the connection is secure or the SSN is encrypted).[235] This section would prevent a bank, for example, from using a customer's SSN as a username, password or personal identification number.[236] Businesses that maintain "computerized data that includes personal information . . . shall notify the owner or licensee of the personal information of a breach of the security of a system if it is likely that the breach has resulted or will result in the misuse of personal information of an individual residing in the State."[237] This notice must be provided as soon as practicable after the breach has been discovered.[238] Finally, the Maryland Code requires state agencies to

---

[228] *See id.* § 10-402(b).
[229] *See* MD. CODE ANN., CRIM. LAW § 93-901(c) (LexisNexis 2010).
[230] *See id.* §93-901(a)(2).
[231] *Id.* § 93-901(e)–(f)(1).
[232] *See id.* § 93-902.
[233] *Id.* § 93-902(a)(3) (limiting private places to a list of more than ten locations).
[234] *See id.* § 93-902(b)(2).
[235] *See* MD. CODE ANN., COM. LAW § 14-3402 (LexisNexis 2010).
[236] *Id.* § 14-3402(a).
[237] *Id.* § 14-3504(c)(1).
[238] *See id.* § 14-3504(c)(2).

adopt and post a privacy policy.[239] The State Government Code states that a state official:[240]

> [W]ho requests personal information for personal records shall provide the following information to each person in interest from whom personal information is collected:
>
> (i) [T]he purpose for which the personal information is collected;
> (ii) [A]ny specific consequences to the person for refusal to provide the personal information; the person's right to inspect, amend, or correct personal records, if any;
> (iii) [W]hether the personal information is generally available for public inspection; and . . .
> (v) [W]hether the personal information is made available or transferred to or shared with any entity other than the official custodian.[241]

The code also states that "[e]ach unit of State government shall post its privacy policies with regard to the collection of personal information, including the policies specified in this subsection, on its Internet website."[242]

U. *Massachusetts*

1. *Electronic Monitoring & Eavesdropping*

Massachusetts law requires the consent of all parties to a wire or oral communication before such communication may be recorded.[243] This provision was passed in order to allow law enforcement to better combat organized crime.[244] Interestingly, a Massachusetts appellate court has also held "that the recorded conversation or communication does not need to be

---

[239] *See* MD. CODE ANN., STATE GOV'T § 10-624 (LexisNexis 2010).
[240] The Maryland Code uses the term official custodian in place of state official. *See id.* § 10-611(d) (stating that "'[o]fficial custodian' means an officer or employee of the State or of a political subdivision who, whether or not the officer or employee has physical custody and control of a public record, is responsible for keeping the public record.").
[241] *Id.* § 10-624(c)(3).
[242] *Id.* § 10-624(c)(4).
[243] *See* MASS GEN. LAWS ch. 272, § 99(B)(4), (C) (2010) (defining an interception, stating that all parties must consent to a legal interception, and stating that "[p]roof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph.").
[244] *Id.* § 99(A).

intelligible in order for the interception to violate the wiretapping statute."[245] Massachusetts does not have any other prominent statutes pertaining to electronic monitoring. This is strange considering that it is one of the few states that has codified an all-parties consent requirement.

V. *Michigan*

1. *Electronic Monitoring & Eavesdropping*

In Michigan, all parties must consent to any eavesdropping of a private conversation. The statute reads as follows:

> Any person who is present or who is not present during a private conversation and who wilfully [sic] uses any device to eavesdrop upon the conversation without the consent of all parties thereto, or who knowingly aids, employs or procures another person to do the same in violation of this section, is guilty of a felony punishable by imprisonment in a state prison for not more than 2 years or by a fine of not more than $2,000.00, or both.[246]

To eavesdrop under Michigan law means "to overhear, record, amplify or transmit any part of the private discourse of others without the permission of all persons engaged in the discourse."[247] The statute applies to eavesdropping whether or not the intercepting individual is a party to the conversation.[248] However, Michigan's eavesdropping statute "has been interpreted by one court as applying only to situations in which a third party has intercepted a communication. This interpretation allows a participant in a conversation to record that conversation without the permission of other parties."[249] That court held that:

> An individual may not expect those he converses with to record their discourses. Still, absent a request that discussions be held "off the record", it is only reasonable to expect that a conversation may be repeated, perhaps from memory or from the handwritten notes of a party to the conversation. A recording made by a participant is nothing more than a more accurate record of what was said.

---

[245] CAN WE TAPE?, *supra* note 41, at Mass.; *see also* Com. v. Wright, 814 N.E.2d 741, 744 (Mass. App. Ct. 2004) (holding that "[i]n effect, the judge indicated, and we agree, that the conversation or communication need not be intelligible, it is enough if isolated words are intelligible.").

[246] MICH. COMP. LAWS § 750.539(c) (2010).

[247] *Id.* § 750.539(a)(2).

[248] *See id.* § 750.539(c).

[249] CAN WE TAPE?, *supra* note 41, at Mich.; *see* Sullivan v. Gray, 324 N.W.2d 58 (Mich. Ct. App. 1982).

> Whether an individual should reasonably expect that an ostensibly private conversation will be related by a participant to third parties depends on that individual's relation to the other participant. The individual may gauge his expectations according to his own evaluation of the person to whom he speaks. He has the ability to limit what he says based upon that expectation. When a third party is unilaterally given permission to listen in upon a conversation, unknown to other participants, those other participants are no longer able to evaluate and form accurate expectations since they are without knowledge of the third party. Therefore, it is not inconsistent to permit a person to record and utilize conversations he participates in yet deny him the right to unilaterally grant that ability to third parties.[250]

In addition, the conversation must be private;[251] the problem is that the statute does not adequately define what constitutes a private conversation. Therefore, Michigan courts have been forced to address the meaning of the phrase. The Michigan Supreme Court has said that "[d]espite the Legislature failing to define 'private conversation' in the eavesdropping statutes, its intent can be determined from the eavesdropping statutes themselves. This is because the Legislature did define the term 'private place.'"[252] A "private place" under Michigan law "means a place where one may reasonably expect to be safe from casual or hostile intrusion or surveillance but does not include a place to which the public or substantial group of the public has access."[253] With this definition in mind, the Michigan Supreme Court stated that a "'private conversation' means a conversation that a person reasonably expects to be free from casual or hostile intrusion or surveillance."[254] The court further held that "although technology provides a means for eavesdropping, the Michigan eavesdropping statutes specifically protect citizens against such intrusions. Therefore, a person is not unreasonable to expect privacy in a conversation although he knows that technology makes it possible for others to eavesdrop on such conversations."[255] This type of wisdom would be very helpful to guide Congress as it revamps the Electronic Communications Privacy Act and its applicability to contemporary monitoring technology.

---

[250] *Sullivan*, 324 N.W.2d at 60–61.
[251] MICH. COMP. LAWS § 750.539(c) (2010).
[252] People v. Stone, 621 N.W.2d 702, 704 (Mich. 2001).
[253] MICH. COMP. LAWS § 750.539(a)(1).
[254] *Stone*, 621 N.W.2d at 704–05.
[255] *Id.* at 706.

2. *Miscellaneous Privacy Protection*

Michigan law prohibits spying on individuals in private places. This means that it is illegal to "[i]nstall, place, or use in any private place, without the consent of the person or persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place."[256] State law allows for the use of RFID technology in state identification cards as long as such technology "is limited to a randomly assigned number which shall be encrypted if agreed to by the department of homeland security, and does not include biometric data."[257] Anyone collecting SSNs "in the ordinary course of business" must create a privacy policy that discusses the use and protection of this information.[258] Employers in Michigan may:

> [N]ot gather or keep a record of an employee's associations, political activities, publications, or communications of nonemployment activities . . . . This prohibition on records shall not apply to the activities that occur on the employer's premises or during the employee's working hours with that employer that interfere with the performance of the employee's duties or duties of other employees.[259]

W. *Minnesota*

1. *Electronic Monitoring & Eavesdropping*

Minnesota law allows one party to a wire, electronic or oral communication to consent to its interception.[260] More specifically, the statute states that it is "not unlawful . . . to intercept a wire, electronic, or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to

---

[256] MICH. COMP. LAWS § 750.539(d)(1)(a).

[257] *Id.* § 28.304(3). Stating that the:

> [S]ecretary of state shall ensure that the radio frequency identification technology is secure from unauthorized data access and includes reasonable security measures to protect against unauthorized disclosure of personal information. An applicant shall be required to sign a declaration acknowledging his or her understanding of the radio frequency identification technology before he or she is issued an enhanced driver license or enhanced official state personal identification card.

Id.

[258] *See id.* § 445.84(1).

[259] *Id.* § 423.508(1).

[260] *See* MINN. STAT. § 626A.02(2)(d) (2010).

such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state."[261]

2. *Miscellaneous Privacy Protection*

Under Minnesota law, an individual commits a gross misdemeanor when the person:

> [S]urreptitiously gazes, stares, or peeps . . . or installs or uses any device for observing, photographing, recording, amplifying, or broadcasting sounds or events . . . . in the window or other aperture of a . . . place where a reasonable person would have an expectation of privacy and has exposed or is likely to expose their intimate parts . . . or the clothing covering the immediate area of the intimate parts; and does so with intent to intrude upon or interfere with the privacy of the occupant.[262]

This prohibition would clearly apply to a locker room and might apply if employers place recording technology in private places such as restrooms and employee offices. However, an employer can argue that the surveillance technology is allowed in vestibules of restrooms and in offices as intimate parts are not likely to be exposed in such areas.

Minnesota law contains an entire section on government data practices. State agencies that collect and use PII must "disclose any breach of the security of the data following discovery or notification of the breach. Notification must be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person."[263] All governmental entities in Minnesota are required to create a privacy policy that describes what types of PII will be collected, how it will be used and secured and how individuals may access such information and consent to its dissemination.[264] Government entities that place cookies on a user's computer must also provide notice to such user as to how PII will be collected, used and disseminated.[265]

---

[261] *Id.*

[262] *Id.* § 609.746(1)(c)–(d).

[263] *Id.* § 13.055(2) (stating that the "disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency . . . or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data").

[264] *See id.* § 13.15(3).

[265] *See id.* (since amended to provide an exception for a cookie temporarily installed by a government entity).

On the employment front, the "employer may not . . . administer a genetic test or request, require, or collect protected genetic information regarding a person as a condition of employment [or] affect the terms or conditions of employment or terminate the employment of any person based on protected genetic information."[266] In addition, "[n]o person shall provide or interpret for any employer or employment agency protected genetic information on a current or prospective employee."[267] The Nonwork Activities section of the Minnesota Code states that an employer "may not refuse to hire a job applicant or discipline or discharge an employee because the applicant or employee engages in or has engaged in the use or enjoyment of lawful consumable products, if the use or enjoyment takes place off the premises of the employer during nonworking hours."[268] The phrase "lawful consumable products" means "products whose use or enjoyment is lawful and which are consumed during use or enjoyment, and includes food, alcoholic or nonalcoholic beverages, and tobacco."[269] While most states prohibit discrimination based on tobacco use only, Minnesota law expands its prohibition to all lawful products.

X. *Mississippi*

1. *Electronic Monitoring & Eavesdropping*

One person to a wire, oral or other communication may consent to its interception in Mississippi.[270] However, the interception may not be "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this state, or for the purpose of committing any other injurious act."[271] An interception under Mississippi law "means the aural or other acquisition of the contents of a wire, oral or other communication through the use of an electronic, mechanical or other device."[272] Individuals who are the victims of these crimes may bring a civil action against the intercepting party.[273] Somewhat awkwardly, Mississippi's wiretapping statute states that:

> This article shall not apply to a person who is a subscriber to a telephone operated by a communication common

---

[266] *Id.* § 181.974(2).
[267] *Id.*
[268] *Id.* § 181.938(2).
[269] *Id.*
[270] *See* MISS. CODE ANN. § 41-29-531(e) (2010) (stating that there is no civil liability for "[a] person not acting under color of law who intercepts a wire, oral or other communication if the person is a party to the communication, or if one (1) of the parties to the communication has given prior consent to the interception").
[271] *Id.* § 41-29-531(e)(1).
[272] *Id.* § 41-29-501(g).
[273] *See id.* § 41-29-529.

> carrier and who intercepts a communication on a telephone to which he subscribes [and this] article shall not apply to persons who are members of the household of the subscriber who intercept communications on a telephone in the home of the subscriber.[274]

It appears that this language is limited to a home telephone line but might also include the telephone lines belonging to an employer.

2. *Miscellaneous Privacy Protection*

Mississippi law states that:

> It shall be unlawful for any public or private employer to require as a condition of employment that any employee or applicant for employment abstain from smoking or using tobacco products during nonworking hours, provided that the individual complies with applicable laws or policies regulating smoking on the premises of the employer during working hours.[275]

Y. *Missouri*

1. *Electronic Monitoring & Eavesdropping*

In Missouri:

> An individual who is a party to a wire communication, or who has the consent of one of the parties to the communication, can lawfully record it or disclose its contents, unless the person is intercepting the communication for the purpose of committing a criminal or tortious act . . . . Recording or disclosing the contents of a wire communication by all other persons is a felony.[276]

Missouri law limits the prohibition to wire communications as opposed to electronic and oral communications.[277] An invasion of privacy in the second degree occurs when an individual "knowingly views, photographs or films another person, without that person's knowledge and consent, while the person being viewed, photographed or filmed is in a state of full or partial nudity and is in a place where one would have a reasonable

---

[274] *Id.* § 41-29-535.
[275] *Id.* § 71-7-33.
[276] CAN WE TAPE?, *supra* note 41, at Mo. (construing MO. REV. STAT. § 542.402 (2010)).
[277] *See id.*

expectation of privacy."[278] This eavesdropping provision would likely only apply in the workplace to restrooms, locker rooms and perhaps walled-off employee offices.

2. *Miscellaneous Privacy Protection*

Missouri makes it a Class A misdemeanor to "require an employee to have personal identification microchip technology implanted into an employee for any reason."[279] This technology is specified as "a subcutaneous or surgically implanted microchip technology device or product that contains or is designed to contain a unique identification number and personal information that can be noninvasively retrieved or transmitted with an external scanning device."[280] Missouri also bans employers from discriminating against employees based on their off-duty consumption of alcohol or tobacco.[281] This is one of the few state statutes that prohibits discrimination based only on alcohol or tobacco. Most lifestyle discrimination statutes ban discrimination based only on tobacco use or more broadly ban discrimination based on all legal off-duty activities. More specifically, the law states that it is an:

> [I]mproper employment practice for an employer to refuse to hire, or to discharge, any individual, or to otherwise disadvantage any individual, with respect to compensation, terms or conditions of employment because the individual uses lawful alcohol or tobacco products off the premises of the employer during hours such individual is not working for the employer, unless such use interferes with the duties and performance of the employee, the employee's coworkers, or the overall operation of the employer's business.[282]

However, employers may provide health insurance benefits at lower rates/deductibles "for employees who do not smoke or use tobacco products."[283] Interestingly, it is not true of employees who consume alcohol but do not smoke or use tobacco products.

---

[278] MO. REV. STAT. § 565.253(1) (2010).
[279] *Id.* § 285.035(1).
[280] *Id.* § 285.035(2).
[281] *Id.* § 290.145.
[282] *Id.*
[283] *See id.*

Z. *Montana*

1. *Constitutional Privacy Protection*

Article II § 10 of the Montana Constitution promulgates a right to privacy. The provision states that "[t]he right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."[284] By its specific terms, this provision is limited to a state action which invades an individual's privacy. The Montana Supreme Court held as much in a case styled *State v. Long*.[285] In *Long*, a private citizen/landlord noticed a light on in his tenant's property; the landlord entered the attic of the property to find marijuana and contacted the authorities who seized the drugs.[286] The court held that this was a private search and that:

> The public policy issue of whether the privacy clause [in the Montana Constitution] *should* cover private action has not been treated in the majority opinion. Rather, we have sought to determine whether there was a clear intention expressed by the framers to depart from traditional constitutional concepts. We found there was not. Therefore, we have limited the application of the privacy clause to state action.[287]

The court also stated that the "battle cry sounded in the dissent [to apply this constitutional protection against invasions by private actors] may, at first blush, have an alluring ring to liberals and civil libertarians. There is, however, a real danger in extending privacy rights to the interaction of individuals."[288]

2. *Electronic Monitoring & Eavesdropping*

In Montana, all parties to a wire communication must consent to its interception. The Privacy in Communications section of the Montana Code makes it unlawful for a person to state that "a person commits the offense of violating privacy in communications if the person knowingly or purposely . . . records or causes to be recorded a conversation by use of a hidden electronic or mechanical device that reproduces a human conversation without the knowledge of all parties to the conversation."[289]

---

[284] MONT. CONST. art. II, § 10.
[285] State v. Long, 700 P.2d 153 (Mont. 1985).
[286] *Id.* at 154.
[287] *Id.* at 167 (Morrison, J., concurring) (emphasis in original).
[288] *Id.*
[289] MONT. CODE ANN. § 45-8-213(c) (2010).

Violation of this provision may result in fines and/or imprisonment for up to six months.[290]

3. *Miscellaneous Privacy Protection*

Employers in Montana may not discriminate against their employees based on such employees' use of lawful products. The relevant section states that "an employer may not refuse to employ or license and may not discriminate against an individual with respect to compensation, promotion, or the terms, conditions, or privileges of employment because the individual legally uses a lawful product off the employer's premises during nonworking hours."[291] The term "lawful products" includes any "product that is legally consumed, used, or enjoyed and includes food, beverages, and tobacco."[292] This lifestyle discrimination statute is more broad than similar statutes in other states which prohibit discrimination based only on tobacco use.

Finally, many Montana governmental agencies are required to post privacy policies. The Montana Governmental Internet Information Privacy Act requires state agencies that collect PII online to ensure that the website:

> (1) [I]dentifies its operator, (2) provides the address and telephone number at which the operator may be contacted as well as an electronic means for contacting the operator; and generally describes the operator's information practices, including policies to protect the privacy of the user and the steps taken to protect the security of the collected information.[293]

In addition:

> [I]f the personally identifiable information may be used for a purpose other than the express purpose of the website or may be given or sold to a third party, except as required by law, then the operator shall ensure that the website includes: a clear and conspicuous notice to the user that the information collected could be used for other than the purposes of the website; a general description of the types of third parties that may obtain the information; and a clear, conspicuous, and easily understood online procedure

[290] *Id.* § 45-8-213(3)(a).
[291] *Id.* § 39-2-313(2).
[292] *Id.* § 39-2-313(1).
[293] *Id.* § 2-17-552(2)–(3).

> requiring an affirmative expression of the user's permission before the information is collected.[294]

Montana law also protects the integrity of PII when the information is subject to a security breach. The state code requires:

> Any person or business that conducts business in Montana and that owns or licenses [or maintains] computerized data that includes personal information [to] disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.[295]

The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[296]

AA. *Nebraska*

1. *Electronic Monitoring & Eavesdropping*

Nebraska law only requires the consent of one party to an electronic, wire or oral communication to consent to its interception.[297] The party to the communication may intercept or authorize a third party to intercept on her behalf.[298] This authorization to intercept is valid unless the interception is "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state."[299]

2. *Miscellaneous Privacy Protection*

Nebraska is one of the few states that requires businesses to adhere to their online PII privacy practices. This PII privacy law is codified in the Deceptive Trade Practices section of the state code. The relevant section states that an individual commits a deceptive trade practice when such person—in the course of a business, vocation or occupation—"[k]nowingly makes a false or misleading statement in a privacy policy, published on the internet or otherwise distributed or published, regarding the use of personal

---

[294] *Id.* § 2-17-552(3).
[295] *Id.* § 30-14-1704(1)–(2).
[296] *Id.* § 30-14-1704.
[297] *See* NEB. REV. STAT. § 86-290(2)(c) (2010).
[298] *See id.*
[299] *Id.*

information submitted by members of the public."[300] The irony with such a prohibition is that individuals and businesses are protected from violating this statute as long as they refrain from posting any privacy policy at all. The only liability comes when they post such a policy and then subsequently violate its terms. A better law would follow California's privacy policy statute and require individuals and businesses that collect PII to actually post a privacy policy. Then, all collectors of PII would be potentially liable for false and misleading statements in their privacy policies. However, Nebraska's law is better than no protection for PII at all—which is the case today in the majority of states.

The Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 protects providers of PII when such information has potentially been compromised. Individuals and businesses that conduct business in Nebraska and own or license PII (or individuals or businesses that maintain PII) referring to Nebraska residents must (1) conduct an investigation when such information might be compromised due to a security breach and (2) provide notice to the affected Nebraska residents if such investigation determines that the PII might be used for unauthorized purposes.[301] Importantly, "[a]ny waiver of the provisions of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 is contrary to public policy and is void and unenforceable."[302]

AB. *Nevada*

1. Electronic Monitoring & Eavesdropping

Nevada's laws surrounding interceptions of electronic communications are both interesting and rather unique. One relevant statute reads: "[e]very person who shall intercept, read or in any manner interrupt or delay the sending of a message over any telephone line shall be guilty of a gross misdemeanor."[303] Another provision states that:

> [I]t is unlawful for any person to intercept or attempt to intercept any wire communication unless: (a) The interception or attempted interception is made with the prior consent of one of the parties to the communication; *and* (b) An emergency situation exists and it is impractical to obtain a court order . . . before the interception.[304]

---

[300] *Id.* § 87-302(a)(14).
[301] *See id.* § 87-803.
[302] *Id.* § 87-805.
[303] NEV. REV. STAT. § 707.900 (2010).
[304] *Id.* § 200.620 (emphasis added).

Therefore, it appears that most instances of wiretapping in Nevada are prohibited. It would be rare for an employer to have an "emergency situation" as required by Nevada law which allows management to monitor employee conversations. It also appears that this consent provision only applies to law enforcement seeking a warrant but not having the time to properly obtain one. Therefore, Nevada courts have held that interception of a wire communication, such as a telephone call, by fewer than all participants involved is prohibited.[305] One Nevada court stated that: "[i]f the legislature had wanted to create that limitation . . . it would have done so. It seems apparent that the legislature believed that intrusion upon Nevadans' privacy by nonconsensual recording of telephone conversations was a greater intrusion than the recording of conversations in person."[306]

Nevada law also holds that:

> [A] person shall not intrude upon the privacy of other persons by surreptitiously listening to, monitoring or recording, or attempting to listen to, monitor or record, by means of any mechanical, electronic or other listening device, any private conversation engaged in by the other persons, or disclose the existence, content, substance, purport, effect or meaning of any conversation so listened to, monitored or recorded, unless authorized to do so by one of the persons engaging in the conversation.[307]

This discussion makes clear that one party may consent to the eavesdropping upon a private oral conversation but that both parties must consent to the interception of a wire communication. Also important is that this statute does not require the conversation to be held in a "private place" as do many other similar state laws.

2. *Miscellaneous Privacy Protection*

Nevada law prohibits employers from discriminating against their employees based on the use of lawful products outside of work hours. The statute clarifies that:

> It is an unlawful employment practice for an employer to: (a) Fail or refuse to hire a prospective employee; or (b) Discharge or otherwise discriminate against any employee concerning his compensation, terms, conditions or privileges of employment, because he engages in the lawful use in this state of any product outside the premises of the employer during his nonworking hours, if that use does not

[305] *See, e.g.*, Lane v. Allstate Ins. Co., 969 P.2d 938, 940–41 (Nev. 1998).
[306] *Id.* at 940.
[307] NEV. REV. STAT. § 200.650 (2010).

> adversely affect his ability to perform his job or the safety of other employees.[308]

The law also states that it is "unlawful for any person, firm or corporation doing business or employing labor in the State of Nevada to make any rule or regulation prohibiting or preventing any employee from engaging in politics or becoming a candidate for any public office in this state."[309]

Nevada also statutorily restricts the fraudulent use of RFID technology. The Nevada Revised Statute states that:

> A person shall not knowingly, intentionally and for the purpose of committing fraud, identity theft or any other unlawful act: (a) Capture, store or read information from the radio frequency identification document of another person without the other person's knowledge and prior consent; or (b) Retain, use or disclose information that the person knows to have been obtained from the radio frequency identification document of another person without the other person's knowledge and prior consent.[310]

AC. *New Hampshire*

1. *Electronic Monitoring & Eavesdropping*

New Hampshire law contains a stricter version of the standard interception statute. In the state, an individual is guilty of a Class B felony if such person, without the consent of all parties to the communication, "[w]ilfully [sic] intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any telecommunication or oral communication."[311] The statute is also violated if an individual:

> Wilfully [sic] uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when . . . such use or endeavor to use (A) takes place on premises of any business or other commercial establishment, or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment.[312]

---

[308] *Id.* § 613.333.
[309] *Id.* § 613.040.
[310] *Id.* § 205.46515.
[311] N.H. REV. STAT. ANN. § 570-A:2(I)(a) (2010).
[312] *Id.* § 570-A:2(I)(b)(3).

Therefore, employers would specifically need the consent of all employees who are monitored when such monitoring occurs on the worksite or involves information relating to the business. Class B felonies in New Hampshire are punishable by one to seven years in prison in addition to any fines which may be imposed.[313] This is one of the most serious incarceration penalties imposed by a state when it comes to illegal interceptions of electronic communications. Interestingly, New Hampshire law makes it only a misdemeanor if only one party to a telecommunication or oral communication consents and the communication is intercepted by a party to the communication or a third party not present.[314]

The law also prohibits eavesdropping, defined as when a person:

> [U]nlawfully and without the consent of the persons entitled to privacy therein, installs or uses . . . [i]n any private place, any device for the purpose of observing, photographing, recording, amplifying or broadcasting, or in any way transmitting images or sounds in such place; or [o]utside a private place, any device for the purpose of hearing, recording, amplifying, broadcasting, or in any way transmitting images or sounds originating in such place which would not ordinarily be audible or comprehensible outside such place.[315]

A private place "means a place where one may reasonably expect to be safe from surveillance including public restrooms, locker rooms, the interior of one's dwelling place, or any place where a person's private body parts including genitalia, buttocks, or female breasts may be exposed."[316]

2. *Miscellaneous Privacy Protection*

New Hampshire law states that "[n]o employer shall require as a condition of employment that any employee or applicant for employment abstain from using tobacco products outside the course of employment, as long as the employee complies with any workplace policy."[317] This is the standard off-duty protection clause, targeted only towards tobacco use, that is found in many other state codes. There is an exception that requires the employee to comply with workplace policy. However, such policies would not legally be allowed to disallow tobacco use specifically. An interesting

---

[313] *See id.* § 570-A:2(I)(a); *id.* § 651:2(II)(b) ("Class B felonies are crimes so designated by statute within or outside this code and any crime defined outside of this code for which the maximum penalty, exclusive of fine, is imprisonment in excess of one year but not in excess of 7 years.").
[314] *Id.* § 570-A:2(I)(a).
[315] *Id.* § 644:9(I)(b)–(c).
[316] *Id.* § 644:9(II).
[317] *Id.* § 275:37(a).

dilemma would occur if such policies attempted to mitigate such use through policies that rewarded "healthy behavior" or something along such lines.

New Hampshire has also enacted a security breach statute that requires, among other things, that any:

> [P]erson doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.[318]

Along these lines, the state has created an RFID Commission to study the use of radio frequency technology in both the public and private sectors.[319] One New Hampshire state statute (with limited exceptions) prohibits the governmental use of RFID technology on state highways to identify the ownership of a motor vehicle or the identity of its occupants.[320]

AD. *New Jersey*

1. *Electronic Monitoring & Eavesdropping*

New Jersey's interception statute bans all purposeful intercepting, or any endeavor to intercept, any wire, electronic or oral communication.[321] There is an exception, however, as long as one party consents before an electronic communication is intercepted, either by a party to such communication or by a third party.[322] More specifically, it is not illegal for:

> A person not acting under color of law to intercept a wire, electronic or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception unless such communication is intercepted or used for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this State or for the purpose of committing any other

---

[318] *Id.* § 359-C:20.
[319] *See, e.g.*, HAROLD CLAMPITT, THE RFID CERTIFICATION TEXTBOOK 419 (American RFID Solutions, Eric C. Jones ed., 3d ed. 2007).
[320] *See* N.H. REV. STAT. ANN. § 236:130 (2010).
[321] *See* N.J. STAT. ANN. § 2A:156A-3 (West 2010).
[322] *Id.* § 2A:156A-4.

> injurious act. The fact that such person is the subscriber to a particular telephone does not constitute consent effective to authorize interception of communications among parties not including such person on that telephone.[323]

This means that employers who do not have the consent of any party to a communication may not legally intercept such communication merely because they provide the telephone line or Ethernet connection. This important privacy protective provision is missing from many other state interception statutes.

2. *Miscellaneous Privacy Protection*

The Labor and Workers Compensation section of the state code declares that no employer:

> [S]hall refuse to hire or employ any person or shall discharge from employment or take any adverse action against any employee with respect to compensation, terms, conditions or other privileges of employment because that person does or does not smoke or use other tobacco products, unless the employer has a rational basis for doing so which is reasonably related to the employment, including the responsibilities of the employee or prospective employee.[324]

This provision is a bit different from the anti-smoking discrimination provisions from other states in that New Jersey employers are allowed to discriminate if they can articulate a "rational basis" that is related to the employment relationship. This allows employers more flexibility than they enjoy in other state smoking discrimination bans. The New Jersey lifestyle discrimination statute also declares that "[n]othing contained in this act shall be construed to affect any applicable laws, rules or workplace policies concerning smoking or the use of other tobacco products during the course of employment."[325]

AE. *New Mexico*

1. *Electronic Monitoring & Eavesdropping*

New Mexico law requires the consent of only one party before a communication may be lawfully intercepted. The Abuse of Privacy chapter in the state code declares that

---

[323] *Id.*
[324] *Id.* § 34:6B-1.
[325] *Id.* § 34:6B-2.

> [I]nterference with communications consists of knowingly and without lawful authority . . . cutting, breaking, tapping or making any connection with any telegraph or telephone line, wire, cable or instrument belonging to or in the lawful possession or control of another, without the consent of such person owning, possessing or controlling such property [or] reading, interrupting, taking or copying any message, communication or report intended for another by telegraph or telephone without the consent of a sender or intended recipient thereof.[326]

2. *Miscellaneous Privacy Protection*

New Mexico's Employee Privacy chapter states that it is unlawful for an employer to:

> Refuse to hire or to discharge any individual, or otherwise disadvantage any individual, with respect to compensation, terms, conditions or privileges of employment because the individual is a smoker or nonsmoker, provided that the individual complies with applicable laws or policies regulating smoking on the premises of the employer during working hours; or
> Require as a condition of employment that any employee or applicant for employment abstain from smoking or using tobacco products during nonworking hours, provided the individual complies with applicable laws or policies regulating smoking on the premises of the employer during working hours.[327]

The provisions of this section:

> [S]hall not be deemed to protect any activity that: materially threatens an employer's legitimate conflict of interest policy reasonably designed to protect the employer's trade secrets, proprietary information or other proprietary interests; or relates to a bona fide occupational requirement and is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees, rather than to all employees of the employer.[328]

---

[326] N.M. STAT. ANN. § 30-12-1 (2010).
[327] *Id.* § 50-11-3.
[328] *Id.*

AF. *New York*

1. *Electronic Monitoring & Eavesdropping*

It is a Class E felony in New York to intercept an electronic communication without the consent of at least one party to such communication.[329] More specifically, the statute bans eavesdropping and defines that concept as follows: "A person is guilty of eavesdropping when he unlawfully engages in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing of an electronic communication."[330] The one-party consent exception, however, comes with the definition of wiretapping. The statute states that '[w]iretapping' means "the intentional overhearing or recording of a telephonic or telegraphic communication by a person other than a sender or receiver thereof, without the consent of either the sender or receiver, by means of any instrument, device or equipment."[331] The code also criminalizes situations where, for no legitimate purpose, a person:

> [I]ntentionally uses or installs, or permits the utilization or installation of an imaging device to surreptitiously view, broadcast or record a person in a bedroom, changing room, fitting room, restroom, toilet, bathroom, washroom, shower or any room assigned to guests or patrons in a motel, hotel or inn, without such person's knowledge or consent.[332]

Employers will always try and argue that their surveillance of a bathroom, changing (locker) room, etc. was made for a legitimate purpose such as during a theft investigation.

2. *Miscellaneous Privacy Protection*

New York law is particularly protective of employee rights outside of the workplace. For example, the New York Labor Code declares that:

> [U]nless otherwise provided by law, it shall be unlawful for any employer or employment agency to refuse to hire, employ or license, or to discharge from employment or otherwise discriminate against an individual in compensation, promotion or terms, conditions or privileges of employment because of . . . an individual's political activities outside of working hours, off of the employer's

---

[329] *See* N.Y. PENAL LAW § 250.00 (McKinney 2010).
[330] *Id.* § 250.50.
[331] *Id.* § 250.00.
[332] *Id.* § 250.45.

> premises and without use of the employer's equipment or other property, if such activities are legal.[333]

This statute places New York in a small minority of states that protect an employee from discrimination based on such employee's political activities. Additionally, employers cannot discriminate against:

> [A]n individual's legal use of consumable products prior to the beginning or after the conclusion of the employee's work hours, and off of the employer's premises and without use of the employer's equipment or other property [or] an individual's legal recreational activities outside work hours, off of the employer's premises and without use of the employer's equipment or other property.[334]

This is one of the broadest state law protections for employee off-duty consumption and activities.

On the information privacy front, New York state law requires that state agencies create privacy policies.[335] More specifically, each:

> [S]tate agency that maintains a state agency website shall adopt an internet privacy policy which shall, at a minimum, include the information required by the [state of New York] model internet privacy policy. Each state agency shall post its internet privacy policy on its website. Such posting shall include a conspicuous and direct link to such privacy policy.[336]

The state code also contains a model internet privacy policy.[337] In addition, the New York code states that:

> No state agency shall collect personal information concerning a user through a state agency website, or disclose personal information concerning a user to any person . . . or other entity, including internal staff who do not need the information in the performance of their official duties . . . unless such user has consented to the collection or disclosure of such personal information. For the purposes of this section, the voluntary disclosure of personal information to a state agency by a user through a state agency website, whether solicited or unsolicited, shall constitute consent to the collection or disclosure of the

---

[333] N.Y. LAB. LAW § 201-d(2) (McKinney 2010).
[334] *Id.* § 201-d(2)(b)–(c).
[335] *See* N.Y. STATE TECH. LAW § 203–204 (McKinney 2010).
[336] *Id.* § 203.
[337] *Id.*

> information by the state agency for the purposes for which the user disclosed it to the state agency, as reasonably ascertainable from the nature and terms of the disclosure.[338]

State agencies that own, license or maintain PII must disclose any breaches to their security systems to any New York resident whose PII is reasonably believed to have been acquired by an unauthorized person.[339] Businesses that own, license, or maintain PII must disclose security breaches where the PII is reasonably believed to have fallen into the hands of an unauthorized individual.[340] Finally, businesses must take care to properly dispose of any records containing PII.[341]

AG. *North Carolina*

1. *Electronic Monitoring & Eavesdropping*

North Carolina law requires that at least one party to an electronic, wire, or oral communication consent to its interception.[342] More specifically, the state code states that "a person is guilty of a Class H felony if, without the consent of at least one party to the communication, the person [w]illfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[343] "In interpreting the meaning of 'consent,' a [North Carolina] appellate court determined that implied consent to interception occurs when one party is warned of monitoring and yet continues with the conversation."[344] In the case of *State v. Price*, the court found that "both parties to the conversation heard the recorded warning that the call was subject to monitoring and recording and that they consented, at least impliedly, by continuing with the conversation in the face of that warning."[345]

2. *Miscellaneous Privacy Protection*

North Carolina law protects most employees in at least some their off-duty activities.[346] The relevant statute applies to both state entities and

---

[338] *See id.* § 204.
[339] *See id.* § 208.
[340] *See* N.Y. GEN. BUS. LAW § 899-aa (McKinney 2010).
[341] *See id.* § 399-h.
[342] *See* N.C. GEN. STAT. § 15A-287 (2010).
[343] *Id.* § 15A-287(a)(1).
[344] CAN WE TAPE?, *supra* note 41, at N.C; *see also* State v. Price, 611 S.E.2d 891, 897 (N.C. Ct. App. 2005).
[345] *See Price*, 611 S.E.2d at 897.
[346] *See* N.C. GEN. STAT. § 95-28.2 (2010).

private entities with at least three regular employees.[347] The provision states that it is:

> [A]n unlawful employment practice for an employer to fail or refuse to hire a prospective employee, or discharge or otherwise discriminate against any employee with respect to compensation, terms, conditions, or privileges of employment because the prospective employee or the employee engages in or has engaged in the lawful use of lawful products if the activity occurs off the premises of the employer during nonworking hours and does not adversely affect the employee's job performance or the person's ability to properly fulfill the responsibilities of the position in question or the safety of other employees.[348]

There are a few key exemptions to this prohibition, the most interesting of which states that it is not an illegal practice to "[r]estrict the lawful use of lawful products by employees during nonworking hours if the restriction relates to the fundamental objectives of the organization."[349] Employers may attempt to argue that having a healthy or health-conscious workforce is a fundamental objective of the organization and thereby attempt to ban smoking outside of business hours. The section does not prohibit an employer from:

> [O]ffering, imposing, or having in effect a health, disability, or life insurance policy distinguishing between employees for the type or price of coverage based on the use or nonuse of lawful products if each of the following is met:
>
> 1. Differential rates assessed employees reflect actuarially justified differences in the provision of employee benefits.
> 2. The employer provides written notice to employees setting forth the differential rates imposed by insurance carriers. [and]
> 3. The employer contributes an equal amount to the insurance carrier on behalf of each employee of the employer.[350]

On the subject of quality of life issues, North Carolina also requires employers to provide up to four hours per year for parents and guardians to

---

[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] *Id.* § 95-28.2(d).

be involved in their child's school.[351] Finally, no "person [or] private entity shall deny or refuse employment to any person or discharge any person from employment on account of the person's having requested genetic testing or counseling services, or on the basis of genetic information obtained concerning the person or a member of the person's family."[352]

On the PII front, businesses must disclose security breaches of PII that they own, license, maintain or possess.[353] Such notice must be clear and conspicuous [and include]:

1. A description of the incident in general terms.
2. A description of the type of personal information that was subject to the unauthorized access and acquisition.
3. A description of the general acts of the business to protect the personal information from further unauthorized access.
4. A telephone number for the business that the person may call for further information and assistance, if one exists.
5. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
6. The toll-free numbers and addresses for the major consumer reporting agencies. [and]
7. The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.[354]

On a separate note, North Carolina state law prohibits state institutions from doing much of anything with an individual's social security number.[355]

AH. *North Dakota*

1. *Electronic Monitoring & Eavesdropping*

Eavesdropping in North Dakota occurs when a person "intentionally intercepts any wire or oral communication by use of any electronic, mechanical, or other device [or] intentionally discloses to any other person

[351] *See* N.C. GEN. STAT. § 95-28.3 (2010).
[352] *Id.* § 95-28.1A.
[353] *See id.* § 75-65.
[354] *Id.* § 75-65(d).
[355] *See id.* § 132-1.10.

or intentionally uses the contents of any wire or oral communication, knowing that the information was obtained through the interception of a wire or oral communication."[356] An intercepting party has a defense to this crime when such individual "was a party to the communication or one of the parties to the communication had given prior consent to such interception, and . . . such communication was not intercepted for the purpose of committing a crime or other unlawful harm."[357] Eavesdropping is classified as a Class C felony under North Dakota law. In addition, "a person is guilty of a class A misdemeanor if he secretly loiters about any building with intent to overhear discourse or conversation therein and to repeat or publish the same with intent to vex, annoy, or injure others."[358] It is unlikely that this provision would be implicated in the employment context as employers monitor employees for reasons such as liability protection, policy enforcement or investigatory purposes. It is harder for an employee-plaintiff to show that an employer monitored in order to vex, annoy or injure another party as required by the statute.

2. *Miscellaneous Privacy Protection*

As of 2007 in North Dakota, a person "may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device. A violation of this section is a class A misdemeanor."[359] This type of prohibition has been slowly appearing in state codes over the past five years likely because someone has actually experienced such an implantation and complained.

The state code also prohibits discrimination based on an employee's lawful off-duty activities as follows:

> It is a discriminatory practice for an employer to fail or refuse to hire a person; to discharge an employee; or to accord adverse or unequal treatment to a person or employee with respect to application, hiring, training, apprenticeship, tenure, promotion, upgrading, compensation, layoff, or a term, privilege, or condition of employment, because of . . . participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer.[360]

---

[356] N.D. CENT. CODE § 12.1-15-02(1)(a)–(b) (2009).
[357] *Id.* § 12.1-15-02(3)(c).
[358] *Id.* § 12.1-15-02(2).
[359] *Id.* § 12.1-15-06.
[360] *Id.* § 14-02.4-03.

This prohibition is stricter than other states' lifestyle discrimination statutes in the fact that: (1) the statute covers more than off-duty tobacco use and (2) the practice at issue must be in "direct conflict" with the employer's business-related interests. A similar statute in Colorado requires less; an employer may discriminate against an employee's off-duty conduct in Colorado as long as the discrimination "[r]elates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular group of employees . . . or [i]s necessary to avoid a conflict of interest with any responsibilities to the employer or the appearance of such a conflict of interest."[361] A reasonable and rational relationship to employment activities as is required in Colorado is much more lenient than a direct conflict as is required in North Dakota. Time will tell whether employers in Colorado take advantage of the state's looser standard while employers in North Dakota find that trying to prohibit employee's off-duty activities is a tougher road to navigate.

AI. *Ohio*

1. *Electronic Monitoring & Eavesdropping*

Ohio law creates a very loose standard when it comes to intercepting a wire, electronic, or oral communication. The relevant statute declares that "[n]o person purposely shall . . . [i]ntercept, attempt to intercept, or procure another person to intercept or attempt to intercept a wire, oral, or electronic communication."[362] An exemption exists when a person:

> [I]ntercepts a wire, oral, or electronic communication, if the person is a party to the communication or if one of the parties to the communication has given the person prior consent to the interception, and if the communication is not intercepted for the purpose of committing a criminal offense or tortious act in violation of the laws or Constitution of the United States or this state or for the purpose of committing any other injurious act.[363]

The "other injurious act" clause of Ohio's prohibition is additional to the standard phraseology from other one-party consent states. The addition of the "other injurious act" phraseology adds more angles for a plaintiff to succeed in a case against an employer for monitoring in the workplace than the plaintiff has if the prohibition is limited to a "criminal offense or tortious act in violation of the laws or Constitution of the United States or [of the state of Ohio]."

---

[361] COLO. REV. STAT. § 24-34-402.5(a)–(b) (2009).
[362] OHIO REV. CODE ANN. § 2933.52(A)(1) (LexisNexis 2010).
[363] *Id.* § 2933.52(B)(4).

AJ. *Oklahoma*

1. *Electronic Monitoring & Eavesdropping*

Oklahoma law requires that only one party to a wire, electronic, or oral communication consent to an interception of such communication. More specifically, it is a felony in Oklahoma when an individual "[w]illfully intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept any wire, oral or electronic communication."[364] This type of violation is punishable by a fine of not less than $5000 and imprisonment of not more than five years, or both.[365] The Acts Not Prohibited section in the same chapter, however, states that:

> [A] person not acting under color of law [may legally] intercept a wire, oral or electronic communication when such person is a party to the communication or when one of the parties to the communication has given prior consent to such interception unless the communication is intercepted for the purpose of committing any criminal act.[366]

Some states also prohibit interception, even with one party's consent, for the purpose of committing tortious acts. Oklahoma has limited this exception to the exception to criminal acts only.

Oklahoma's eavesdropping statute states that "[e]very person guilty of secretly loitering about any building, with intent to overhear discourse therein, and to repeat or publish the same to vex, annoy, or injure others, is guilty of a misdemeanor."[367] It would be interesting to determine whether this provision could be used against an employer who monitors employees by loitering outside of their offices. The likelihood is that such actions would be legal under this statute as management would likely to make a strong case that the eavesdropping was not meant to vex, annoy, or injure employees. This statute, by its express terms, seems limited to the overhearing of communications without the assistance of monitoring technology.

2. *Miscellaneous Privacy Protection*

Oklahoma law states that "[n]o person, state, county, or local governmental entity or corporate entity may require an individual to undergo the implanting of a microchip or permanent mark of any kind or

---

[364] OKLA. STAT. tit. 13, § 176.3(1) (2010).
[365] *See id.*
[366] *Id.* § 176.4(5).
[367] *Id.* at tit. 21, § 1202.

nature upon the individual."[368] For violations if this provision, the Oklahoma Department of Health "may impose a fine not to exceed Ten Thousand Dollars ($10,000) on any person who violates this act. Each day of continued violation shall constitute a separate offense."[369] In addition, Oklahoma has its own lifestyle discrimination statute. The relevant section declares that employers may not:

> Discharge any individual, or otherwise disadvantage any individual, with respect to compensation, terms, conditions or privileges of employment because the individual is a nonsmoker or smokes or uses tobacco products during nonworking hours; or [r]equire as a condition of employment that any employee or applicant for employment abstain from smoking or using tobacco products during nonworking hours."[370]

AK. *Oregon*

1. *Electronic Monitoring & Eavesdropping*

The state of Oregon allows one party to consent to the interception of a wire or oral communication. In the words of the relevant statute:

> [A]ny person who willfully intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept any wire or oral communication where such person is not a party to the communication and where none of the parties to the communication has given prior consent to the interception, is guilty of a Class A misdemeanor."[371]

In addition, except as authorized in the state wiretapping statute, a person may not "[o]btain or attempt to obtain the whole or any part of a conversation by means of any device, contrivance, machine or apparatus, whether electrical, mechanical, manual or otherwise, if not all participants in the conversation are specifically informed that their conversation is being obtained."[372] This section of the Oregon Code would prohibit employers who are not a party to a communication from obtaining a recording of their employees without the consent of all parties to the communication.

---

[368] *Id.* at tit. 63, § 1-1430(A).
[369] *Id.* at tit. 63, § 1-1430(B).
[370] *Id.* at tit. 40, § 500.
[371] OR. REV. STAT. § 165.543(1) (2009).
[372] *Id.* § 165.540(1)(c).

2. *Miscellaneous Privacy Protection*

The Oregon Code is very protective when it comes to privacy surrounding an employee's religious and political viewpoint. For example, Oregon law states that:

> An employer . . . may not discharge, discipline or otherwise penalize or threaten to discharge, discipline or otherwise penalize or take any adverse employment action against an employee . . . [b]ecause the employee declines to attend or participate in an employer-sponsored meeting or communication with the employer . . . if the primary purpose of the meeting or communication is to communicate the opinion of the employer about religious or political matters."[373]

This statute is designed to hinder employer efforts to pressure employees to toe the party line when it comes to the political or religious stance of management. This provision becomes particularly interesting in cases where politics and ideology may play a major role in an organization's culture. For example, political leanings often play a role in various institutions of higher education and such stances can create discomfort for employees with differing belief systems. On the other hand, violations of this statute might be rare as management's positions on politics and religion are generally passed along subtly via the organizational culture rather than discussed at employer-sponsored meetings.

Interestingly, Oregon law contains a related statute that reads:

> If an employer requires an applicant or employee to have an academic degree from a post-secondary institution to qualify for a position, but does not require a degree with a specific title, it is an unlawful employment practice for the employer to refuse to hire or promote or in any manner discriminate or retaliate against the applicant or employee only because the applicant or employee meets the educational requirements for the position by having a degree with a title in theology or religious occupations from a school that, when the degree was issued, was a school described in [the Education chapter of the state code].[374]

This provision helps to reduce discrimination against religion in the hiring process.

---

[373] *Id.* § 659.785.
[374] *Id.* § 659A.318.

Finally, Oregon's lifestyle discrimination statute declares that it is "an unlawful employment practice for any employer to require, as a condition of employment, that any employee or prospective employee refrain from using lawful tobacco products during nonworking hours, except when the restriction relates to a bona fide occupational requirement."[375] This is standard language for a lifestyle discrimination statute prohibiting discrimination based on an employee's off-duty tobacco use.

AL. *Pennsylvania*

1. *Electronic Monitoring & Eavesdropping*

Pennsylvania law is one of the rare states that requires all parties to consent to the interception of an electronic, wire, or oral communication.[376] More specifically, the relevant statute declares that: "It shall not be unlawful and no prior court approval shall be required under this chapter for . . . [a] person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception."[377]

2. *Miscellaneous Privacy Protection*

Pennsylvania laws states that it is a deceptive or fraudulent business practice for a person–in the course of business–to "knowingly make a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."[378] As stated previously, the major problem with such privacy policy requirements is that businesses are not required to post a policy in the first place. In fact, if a business does post a privacy policy, then it may be held liable for any breach of privacy policy terms. If a business strategically chooses not post a privacy policy, management has proposed no terms to breach and cannot be held liable for the ways they collect, use and disseminate PII. Again, this type of statute is better than no privacy policy statute at all–but it could be strengthened by requiring all businesses that collect, use, store, or disseminate PII to at least post a policy. Then, consumers will understand how their PII is treated and may choose not to submit. In addition, companies will be liable for breaching privacy policy terms.

Pennsylvania also has a security breach notification law that states:

---

[375] *Id.* § 659A.315.
[376] *See* 18 PA. CONS. STAT. § 5703 (2010).
[377] *Id.* § 5704(4).
[378] *Id.* § 4107(10).

> An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided . . . or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.[379]

AM. *Rhode Island*

1. *Electronic Monitoring & Eavesdropping*

Rhode Island law provides that "any person who willfully intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept, any wire, electronic, or oral communication . . . shall be imprisoned for not more than five (5) years."[380] One exception to this prohibition states that it is not unlawful for:

> A person not acting under color of law to intercept a wire, electronic, or oral communication, where the person is a party to the communication, or one of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in the violation of the constitution or laws of the United States or of any state or for the purpose of committing any other injurious act."[381]

The Supreme Court of Rhode Island "has also stated that Rhode Island's wiretapping laws should be interpreted more strictly than federal wiretapping statutes 'in the interest of giving the full measure of protection to an individual's privacy.'"[382]

---

[379] 73 PA. CONS. STAT. ANN. § 2303 (West 2010).
[380] R.I. GEN. LAWS § 11-35-21(a) (2009).
[381] *Id.* § 11-35-21(c)(3).
[382] CAN WE TAPE? *supra* note 41, at R.I. (quoting State v. O'Brien, 774 A.2d 89, 100 (R.I. 2001)).

2. *Miscellaneous Privacy Protection*

The Rhode Island Identity Theft Protection Act of 2005 states that a "business that owns or licenses computerized unencripted [sic] personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[383] In addition:

> A business that discloses computerized unencripted [sic] personal information about a Rhode Island resident pursuant to a contract with a nonaffiliated third-party shall require by contract that the third-party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[384]

These PII protection provisions are likely to go a long way in protecting such information from making its way to the open market. It is doubtful that a purchaser of PII who desires to sell such information would be interested in signing a contract promising to secure the same data it wishes to disseminate. In addition, the state also has the standard security breach notification statute that applies to both state agencies and individuals.[385]

AN. *South Carolina*

1. *Constitutional Privacy Protection*

Article I, Section 10 of the South Carolina constitution creates a right to privacy. The relevant section states that:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures *and unreasonable invasions of privacy* shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.[386]

This provision has been held to only apply to invasions of privacy by state actors as opposed to private parties. For example, in *Southern Bell*

---

[383] R.I. GEN. LAWS §11-49.2-2(2) (2009).
[384] *Id.* § 11-49.2-112(3).
[385] *Id.* § 11-49.2-3.
[386] S.C. CONST. art. I, § 10 (emphasis added).

Telephone and Telegraph Company v. Hamm, the South Carolina Supreme Court held:

> Before deciding whether the [Caller ID service behind the alleged invasion of privacy in the case] is violative of constitutional rights of privacy, however, we must first determine that the actions of the South Carolina PSC rose to the level of 'state action' as, absent that involvement, the constitutional right to privacy does not attach."[387]

In addition, "[t]hough article I, section 10 of the South Carolina Constitution contains an explicit reference to the word 'privacy,' the word is no more than an addendum to the search and seizure provision and has been interpreted as such."[388]

2. *Electronic Monitoring & Eavesdropping*

South Carolina law requires that only one party need to consent to the interception of a wire, electronic or oral communication for such interception to be lawful.[389] The statute begins differently than similar provisions in other jurisdictions stating that the "interception of wire, electronic, or oral communications is hereby authorized only in the manner permitted by this chapter."[390] The chapter then makes it illegal to intercept, use or disclose any wire, electronic or oral communication unless, among other things, "a person not acting under color of law . . . intercept[s] a wire, oral, or electronic communication where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception."[391]

As opposed to its less privacy protective one-party consent interception provision, South Carolina has a more robust eavesdropping—or Peeping Tom as it is called in the state code—statute. The language of the Peeping Tom statute reads:

> It is unlawful for a person to be an eavesdropper or a peeping tom on or about the premises of another or to go upon the premises of another for the purpose of becoming an eavesdropper or a peeping tom. The term "peeping tom", as used in this section, is defined as a person who peeps through windows, doors, or other like places, on or about the premises of another, for the purpose of spying

---

[387] S. Bell Tel. & Tel. Co. v. Hamm, 409 S.E.2d. 775, 778 (S.C. 1991).
[388] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1142 (Summer 2002).
[389] S.C. CODE ANN. § 17-30-30(C) (2009).
[390] *Id.* § 17-30-10.
[391] *Id.* § 17-30-30(C).

> upon or invading the privacy of the persons spied upon and any other conduct of a similar nature, that tends to invade the privacy of others. The term "peeping tom" also includes any person who employs the use of video or audio equipment for the purposes set forth in this section. A person who violates the provisions of this section is guilty of a misdemeanor and, upon conviction, must be fined not more than five hundred dollars or imprisoned not more than three years, or both.[392]

The code recognizes that the twenty-first century Peeping Tom can monitor with sophisticated technology as well as with the naked eye and covers technology in this statute as well. The statute defines a "place where a person would have a reasonable expectation of privacy" as "a place where a reasonable person would believe that he or she could disrobe in privacy, without being concerned that his or her undressing was being photographed, filmed, or videotaped by another; or a place where one would reasonably expect to be safe from hostile intrusion or surveillance."[393] Under this prohibition, plaintiff-employees must prove that they were in a private place and that their employer monitored their activities in a manner that constituted spying or an invasion of privacy. The invasion of privacy torts would likely be a good guide as to what constitutes an invasion of privacy under this statute.

3. *Miscellaneous Privacy Protection*

South Carolina law states that the "use of tobacco products outside the workplace must not be the basis of personnel action, including, but not limited to, employment, termination, demotion, or promotion of an employee."[394] It is important to remember that these types of lifestyle discrimination statutes are modifications to the employment at will rule.

The state code has an entire section titled Personal Identifying Information Privacy Protection. The South Carolina General Assembly found that:

> Although there are legitimate reasons for state and local government entities to collect social security numbers and other personal identifying information from individuals, government entities should collect the information only for legitimate purposes or when required by law. An entity that provides employee benefits has a legitimate need to collect and use social security numbers and personal

[392] *Id.* § 16-17-470(A).
[393] *Id.* § 16-17-470(D)(1)(a)–(b).
[394] *Id.* § 41-1-85.

> identifying information as part of its administration and provision of employee benefits programs.[395]

The Assembly also found that when "state and local government entities possess social security numbers or other personal identifying information, the governments should minimize the instances this information is disseminated either internally within government or externally with the general public."[396] With this finding in mind, a state statute requires that state agencies collecting SSNs adhere to nine specific personal information privacy requirements (in addition to the proper and safe disposal of SSN data).[397] Similar restrictions also apply to the use of SSNs by private parties such as businesses.[398] The code also limits the manner in which PII may be disseminated.[399] Finally:

> All state agencies, boards, commissions, institutions, departments, and other state entities, by whatever name known, must develop privacy policies and procedures to ensure that the collection of personal information pertaining to citizens of the State is limited to such personal information required by any such agency, board, commission, institution, department, or other state entity and necessary to fulfill a legitimate public purpose.[400]

If the state agency "hosts, supports, or provides a link to page or site accessible through the world wide web, [it] must clearly display its privacy policy and the name and telephone number of the agency, board, commission, institution, department, or other state entity person responsible for administration of the policy."[401] The section concludes by stating that "[w]here personal information is authorized to be collected by an entity covered by this section, the entity must at the time of collection advise the citizen to whom the information pertains that the information is subject to public scrutiny or release."[402]

---

[395] *Id.* § 30-2-300(2).
[396] *Id.* § 30-2-300(3).
[397] *Id.* § 30-2-310(A)(1)(a)–(i), (C).
[398] *See id.* § 37-20-180.
[399] *See id.* § 30-2-320.
[400] *Id.* § 30-2-20.
[401] *Id.* § 30-2-40(A).
[402] *Id.* § 30-2-40(B).

AO. *South Dakota*

1. *Electronic Monitoring & Eavesdropping*

In South Dakota, one party to a communication may intercept, or authorize a third party to intercept, the communication.[403] The pertinent statute declares that a person is guilty of a Class 5 felony if he is not a sender or receiver of a "telephone or telegraph communication [and] intentionally and by means of an eavesdropping device overhears or records a telephone or telegraph communication, or aids, authorizes, employs, procures, or permits another to so do, without the consent of either a sender or receiver thereof."[404] The same is true if a person is "not present during a conversation or discussion [and] intentionally and by means of an eavesdropping device overhears or records such conversation or discussion, or aids, authorizes, employs, procures, or permits another to so do, without the consent of a party to such conversation or discussion."[405] These two provisions, by their express terms, exempt the sender and receiver of a communication as well as a third party interceptor from punishment for intercepting. This statute is similar to the federal requirement but is not drafted in the same manner.

The Invasion Of Privacy section of the South Dakota code states that it is a Class One misdemeanor when a person "[i]nstalls in any private place, without the consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in such place, or uses any such unauthorized installation."[406] Sexual desire or gratification is not an element in this statute making it much more applicable to the employment context.

2. *Miscellaneous Privacy Protection*

South Dakota law states:

> It is a discriminatory or unfair employment practice for an employer to terminate the employment of an employee due to that employee's engaging in any use of tobacco products off the premises of the employer during nonworking hours unless such a restriction:
>
> (1) Relates to a bona fide occupational requirement and is reasonably and rationally related to the employment activities and responsibilities of a

[403] *See* S.D. CODIFIED LAWS § 23A-35A-20 (2010).
[404] *Id.* § 23A-35A-20(1).
[405] *Id.* § 23A-35A-20(2).
[406] *Id.* § 22-21-1(2).

> particular employee or a particular group of employees, rather than to all employees of the employer; or
>
> (2) Is necessary to avoid a conflict of interest with any responsibilities to the employer or the appearance of such a conflict of interest.[407]

AP. *Tennessee*

1. *Electronic Monitoring & Eavesdropping*

Under Tennessee Law:

> It is lawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication, where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the state of Tennessee.[408]

If no party to the communication consents, then an interception by a third party (not acting under the color of law) would likely be illegal.

On the eavesdropping front, Tennessee's Observation Without Consent statute declares:

> It is an offense for a person to knowingly spy upon, observe or otherwise view an individual, when the individual is in a place where there is a reasonable expectation of privacy, without the prior effective consent of the individual, if the viewing [w]ould offend or embarrass an ordinary person if the person knew the person was being viewed [and was] for the purpose of sexual arousal or gratification of the defendant.[409]

The sexual arousal or gratification requirements of this section likely prohibit its use in all but the worst employer monitoring cases.

---

[407] *Id.* § 60-4-11.
[408] TENN. CODE ANN. § 39-13-601 (2010).
[409] *Id.* § 39-13-607(a)(1)–(2).

2. *Miscellaneous Privacy Protection*

Tennessee law prohibits employers from discriminating against employees based on employee use of agricultural products. More specifically, the statute states that:

> No employee shall be discharged or terminated solely for participating or engaging in the use of an agricultural product not regulated by the alcoholic beverage commission that is not otherwise proscribed by law, if the employee participates or engages in the use in a manner that complies with all applicable employer policies regarding the use during times at which the employee is working.[410]

This is the only lifestyle discrimination statute that looks at off-duty employee consumption of agricultural products as opposed to the consumption of alcohol or tobacco specifically.

The Tennessee Identity Theft Deterrence Act of 1999 (ITDA) contains security breach provisions very similar to other states that protect PII after it has been accessed inappropriately.[411] The ITDA also requires individuals and businesses to adequately protect SSNs.[412] The relevant part of the statute concerning reads as follows:

> On and after January 1, 2008, any person, nonprofit or for profit business entity in this state . . . that has obtained a federal social security number for a legitimate business or governmental purpose shall make reasonable efforts to protect that social security number from disclosure to the public. Social security numbers shall not:
>
> (1) Be posted or displayed in public;
> (2) Be required to be transmitted over the Internet, unless the Internet connection used is secure or the social security number is encrypted;
> (3) Be required to log onto or access an Internet website, unless used in combination with a password or other authentication device;
> (4) Be printed on any materials mailed to a consumer, unless the disclosure is required by law, or the document is a form or application; or
> (5) Be printed on any card, identification or badge that the consumer must display or present in order to

[410] *Id.* § 50-1-304(e)(1).
[411] *Id.* § 47-18-2107.
[412] *Id.* § 47-18-2110.

> receive a benefit, good, service or other thing of value to which the consumer is entitled based upon the consumer's contract or other agreement with the entity issuing the card, identification or badge.[413]

Finally, Tennessee is one of a few states that require employers—in this case state agency employers—to provide notice of e-mail monitoring practices. More specifically, the statute reads that:

> On or before July 1, 2000, the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system shall adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted .... The policy shall include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection under this part.[414]

The statute requires such notice even if no monitoring is scheduled to take place. Perhaps a state agency could argue that it will never monitor employee e-mail and, therefore, that it does not need a policy. However, such a stance could easily be disclosed in a policy and would likely be morale-boosting.

AQ. *Texas*

1. *Electronic Monitoring & Eavesdropping*

In Texas:

> So long as a wire, oral, or electronic communication—including the radio portion of any cordless telephone call—is not recorded for a criminal or tortious purpose, anyone who is a party to the communication, or who has the consent of a party to the communication . . . can lawfully record the communication and disclose its contents.[415]

The cordless telephone situation mentioned in the statute arises often in wiretapping cases where defendants claim that the use of a cordless phone indicates that the user did not have a reasonable expectation of privacy.

---

[413] *Id.* § 47-18-2110(a)(1)–(5).
[414] *Id.* § 10-7-512 (2010).
[415] CAN WE TAPE?, *supra* note 41, at Tex. (citing TEX. PENAL CODE ANN. § 16.02 (West 2010)).

Texas is one of the few states that expressly includes a cordless phone provision in its wiretapping statute. This helps alleviate the court system from dealing with wiretapping cases stemming from cordless phone use.

2. *Miscellaneous Privacy Protection*

Texas law allows the State Department of Transportation to insert RFID chips into state identification cards but requires that such information gained be encrypted or secured from unauthorized access.[416] For example, "[a] person [not only state agencies but any person] may not sell or otherwise disclose biometric information accessed from an enhanced driver's license or any information from an enhanced driver's license radio frequency identification chip or similar technology to another person or an affiliate of the person."[417] This provision indicates that Texas has chosen to prohibit PII skimming legislatively instead of relying on invasion of privacy tort cases.

The Texas code also states that a person "may not require an individual to disclose the individual's social security number to obtain goods or services from or enter into a business transaction with the person unless the person [adopts a privacy policy dealing with the use of SSNs."[418] On the governmental front, state agencies in Texas are required to create and post a privacy policy that:

> (1) prescribes terms under which a person may use, copy information from, or link to a generally accessible Internet site maintained by or for a state agency; and
> (2) protects the personal information of members of the public who access information from or through a generally accessible Internet site maintained by or for a state agency.[419]

Additionally, a governmental agency is required to "prominently post a link to the policy statement on a generally accessible Internet site maintained by or for the agency."[420]

---

[416] TEX. TRANSP. CODE ANN. § 521.032(c) (West 2007).
[417] *Id.* § 521.032(g).
[418] *Id.* § 501.052.
[419] TEX. GOV'T CODE ANN. § 2054.126(a)(1)–(2).
[420] *Id.* § 2054.126(b).

AR. *Utah*

1. *Electronic Monitoring & Eavesdropping*

Utah state law requires that one party may legally consent to the interception of a wire, electronic or oral communication.[421] Located with the Utah Code of Criminal Procedure, the relevant statute states that it is a third degree felony when a person "intentionally or knowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic, or oral communication."[422] This is the standard wiretapping prohibition found in federal law. One of the exceptions states that:

> [An intercepting person] not acting under color of law may intercept a wire, electronic, or oral communication if that person is a party to the communication or one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of state or federal laws.[423]

Utah has also enacted an eavesdropping statute. The pertinent part of the statute states that a person commits a Class B misdemeanor when he:

> (A) Trespasses on property with intent to subject anyone to eavesdropping or other surveillance in a private place; or
>
> (B) Installs in any private place, without the consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying, or broadcasting sounds or events in the place or uses any such unauthorized installation; or
>
> (C) Installs or uses outside of a private place any device for hearing, recording, amplifying, or broadcasting sounds originating in the place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy there.[424]

A "private place" is defined under Utah law as "a place where one may reasonably expect to be safe from casual or hostile intrusion or surveillance."[425] Under Utah's eavesdropping statute, an employee might

---

[421] UTAH CODE ANN. § 77-23a-4(7)(a)–(b) (LexisNexis 2010).
[422] *Id.* § 77-23a-4(1)(b)(i).
[423] *Id.* § 77-23a-4(7)(b).
[424] *Id.* § 76-9-402.
[425] *Id.* § 76-9-401(1).

have a claim that she possessed a reasonable expectation that she would be safe from casual and hostile surveillance in her workplace office. The claim would be less strong in a work cubicle or in the hallways, as these areas are less likely to be categorized as private places.

2. *Miscellaneous Privacy Protection*

Utah has a unique chapter in its state code titled the Notice of Intent to Sell Nonpublic Personal Information Act. This act states that a commercial entity shall provide notice to a consumer if:

> (i) The commercial entity enters into a consumer transaction with that person;
> (ii) As a result of the consumer transaction . . . the commercial entity obtains nonpublic personal information concerning that person; and
> (iii) The commercial entity intends to or wants the ability to disclose the nonpublic personal information:
> (A) to a third party; and
> (B) for compensation."[426]

These types of situations occur often in the world of PII collection. Businesses often find that collected PII is useful not only to complete business transactions but also to sell on the open market. If a business in Utah chooses to disseminate PII, the state code has rules for when such dissemination requires disclosure. In transactions requiring disclosure, the compensation paid to the seller must be "(A) . . . the primary consideration for the commercial entity disclosing the nonpublic personal information; (B) . . . directly related to the commercial entity disclosing the nonpublic personal information; and (C) . . . not compensation received by the commercial entity in consideration of a transaction."[427] This type of statute will likely prevent businesses from selling PII to avoid providing this type of notice to customers. At the same time, this statute limits a PII use that is valid in most every other state and on the federal level.

On the state government side of the equation, Utah's Governmental Internet Information Privacy Act states that:

> A governmental entity may not collect personally identifiable information related to a user of the governmental entity's governmental website unless the governmental entity has taken reasonable steps to ensure that on the day on which the personally identifiable information is collected the governmental entity's

[426] *Id.* § 13-37-201(1)(a)(i)–(iii).
[427] *Id.* § 13-37-201(1)(a)(iv)(A)–(C).

governmental website [contains a privacy policy with six required components.][428]

AS. *Vermont*

1. *Electronic Monitoring & Eavesdropping*

Vermont law on the topic of electronic monitoring and eavesdropping in the workplace is rather unique. It is unique in the fact that there "are no specific statutes in Vermont addressing interception of communications [although] the state's highest court has held that surreptitious electronic monitoring of communications in a person's home is an unlawful invasion of privacy."[429] Vermont is the only state that has not enacted either a one-party or two-party consent statute. The state assembly has likely decided that tort law and precedent is sufficient to handle potential invasions of privacy stemming from wiretapping.

2. *Miscellaneous Privacy Protection*

On the RFID front, Vermont law requires a radio frequency identification device to be implanted in a state identification card (i.e., driver's license). More specifically, the law states, among other things, that the "face of an enhanced license shall contain the individual's name, date of birth, gender, a unique identification number, full facial photograph or imaged likeness [and a] *vicinity Radio Frequency Identification chip shall be embedded in the enhanced license in compliance with the security standards of the Department of Homeland Security.*"[430] Any additional personal identity information not currently required by the Department of Homeland Security "shall need the approval of either the general assembly or the legislative committee on administrative rules prior to the implementation of the requirements."[431] This data is supposed to remain reasonably secure as Vermont law states that no "person shall compile or maintain a database of electronically readable information derived from an operator's license."[432] The law also states that personal radio frequency identification chip numbers "shall be given protections as codified in [the federal Drivers Privacy Protection Act]."[433]

---

[428] *Id.* § 63D-2-103(1)–(2).
[429] CAN WE TAPE?, *supra* note 41, at Vt.
[430] VT. STAT. ANN. tit. 23, § 7 (2010) (emphasis added).
[431] *Id.*
[432] *Id.* § 7(c).
[433] *Id.* § 8 (emphasis added).

AT. *Virginia*

1. *Electronic Monitoring & Eavesdropping*

Virginia law allows one party to consent to the interception of a wire, electronic, or oral communication. In fact, it is a Class 6 felony in the state when a person "[i]ntentionally intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept, any wire, electronic or oral communication."[434] The code then grants an exception to the rule stating that it "shall not be a criminal offense under this chapter for a person to intercept a wire, electronic or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[435] This statute does not add the extra provisions, which state that, regardless of consent, an interception may not occur for criminal and/or tortious purposes. Perhaps other chapters in the state's penal code would deal with such situations.

2. *Miscellaneous Privacy Protection*

The Virginia state code provides that the Department of Motor Vehicles "shall not comply with any federal law or regulation that would require the Department to use any type of computer chip or radio-frequency identification tag or other similar device on or in a driver's license or special identification card."[436] This provision is 180 degrees different from those of other states—such as Vermont—that actually require the use of RFID chips in driver's licenses.

Along these lines, Virginia take steps to protect an individual's PII that has been collected by a third party from misuse and from falling into the wrong hands. The General Assembly of Virginia made findings that:

> 1. An individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;
> 2. The increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;
> 3. An individual's opportunities to secure employment, insurance, credit, and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and

[434] VA. CODE ANN. § 19.2-62(A)(1) (2010).
[435] *Id.* § 19.2-62(B)(2).
[436] *Id.* § 46.2-323.01.

> 4. In order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.[437]

With these privacy protective findings in mind, all Virginia state agencies that create Web sites are required to create and post privacy policies that discuss how such information is handled.[438] More specifically:

> Every public body . . . that has an Internet website associated with that public body shall develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public . . . . The statement shall be made available on the public body's website in a conspicuous manner. The Secretary of Technology or his designee shall provide guidelines for developing the policy and the statement, and each public body shall tailor the policy and the statement to reflect the information practices of the individual public body. At minimum, the policy and the statement shall address (i) what information, including personally identifiable information, will be collected, if any; (ii) whether any information will be automatically collected simply by accessing the website and, if so, what information; (iii) whether the website automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and (iv) how the collected information is being used or will be used.[439]

In addition to the privacy policy requirement, the state code also provides more specific protection for individuals when state agencies collect their PII.[440] This is necessary because the privacy policy provision only requires that state agencies declare how PII will be collected and handled. The relevant PII protection statute reads that "it shall be unlawful for any agency to disclose the social security number or other identification numbers appearing on driver's licenses or information on credit cards, debit cards, bank accounts, or other electronic billing and payment systems that was supplied to an agency for the purpose of paying fees, fines, taxes, or other charges collected by such agency."[441]

---

[437] *Id.* § 2.2-3800.
[438] *Id.* § 2.2-3803(10)(B).
[439] *Id.*
[440] *See id.* § 2.2-3808.
[441] *Id.* § 2.2-3808.1 (2010); *see also id.* § 2.2-3815 (requiring that the first five digits of a SSN in a public record remain private and secure from disclosure).

AU. *Washington*

1. *Constitutional Privacy Protection*

The state of Washington takes PII privacy more seriously than most of the other state codes. This occurs primarily through each of the following restrictions: (1) an all-party consent requirement for wiretapping, (2) a requirement that government agencies protect PII held on RFID chips and (3) strong protections against invasions of privacy based on the disclosure of information contained in public records. Somewhat important is the right to privacy contained in Article I, Section 7 of the state constitution. This provision states that: "*No person shall be disturbed in his private affairs*, or his home invaded, without authority of law."[442] Although this provision does not state that only invasions caused by state actors are prohibited, precedent makes the case very clearly. For example, a 1986 case styled *Trumbauer v. Group Health Cooperative of Puget Sound* held that both clauses of this constitutional provision may only be violated via state action.[443] In its own words, the court held that the "due process and search and seizure provisions of the Washington State Constitution apply only to state action. Trumbauer's claims under these provisions must be dismissed because Trumbauer's allegations present a purely private dispute."[444] With this state action requirement in mind, individuals experiencing privacy invasions from private actors/businesses as well as employees working in the private sector gain little protection from this section of the Washington Constitution.

2. *Electronic Monitoring & Eavesdropping*

In Washington, all parties to a private communication must consent to its interception.[445] The state code makes it unlawful for any individual, [business,] . . . or the state of Washington . . . to intercept, or record any:

> (a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the

[442] WASH. CONST. art. I, § VII (emphasis added).
[443] Trumbauer v. Grp. Health Co-op. of Puget Sound, 635 F. Supp. 543, 549 (W.D. Wash. 1986).
[444] *Id.* (internal citations omitted).
[445] WASH. REV. CODE § 9.73.030(1)(b) (2010).

> consent of all the participants in the communication;
>
> (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation.[446]

The word private is inserted before the terms communication and conversation in Washington's wiretapping/eavesdropping statute. This likely restricts interceptions to communications where parties have a reasonable expectation of privacy. However, the "all-party consent requirement can be satisfied if 'one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted.'"[447] This required announcement would make it impossible for employers to covertly monitor a communication between two or more employees to which the employer either was or was not a participant. In addition, "if the conversation is to be recorded, the requisite announcement must be recorded as well."[448]

3. *Miscellaneous Privacy Protection*

Washington law delineates the requirements necessary for an individual to obtain a driver's license or a state identification card (called an identicard in Washington).[449] As part of this process, the state code also requires that the "enhanced driver's license or identicard must include reasonable security measures to protect the privacy of Washington state residents, including reasonable safeguards to protect against unauthorized disclosure of data about Washington state residents."[450] If the enhanced driver's license or identicard "includes a radio frequency identification chip, or

---

[446] *Id.* § 9.73.030(1)(a)–(b).

[447] CAN WE TAPE?, *supra* note 41, at Wash. (citing WASH. REV. CODE § 9.73.030 (2010)).

[448] *Id.*

[449] *See* WASH. REV. CODE § 46.20.117 (2010).

[450] *Id.* § 46.20.202; *see also id.* § 42.56.330(8). Stating that the:

> [P]ersonally identifying information of persons who acquire and use a driver's license or identicard that includes a radio frequency identification chip or similar technology to facilitate border crossing . . . may be disclosed in aggregate form as long as the data does not contain any personally identifying information. Personally identifying information may be released to law enforcement agencies for other purposes only if the request is accompanied by a court order.

Id.

similar technology, the department shall ensure that the technology is encrypted or otherwise secure from unauthorized data access."[451] It is also a crime under Washington law to use RFID technology to skim (i.e., intercept) PII from an individual's identification documents. More specifically, Washington law states that "a person is guilty of a class C felony if the person intentionally possesses, or reads or captures remotely using radio waves, information contained on another person's identification document, including the unique personal identifier number encoded on the identification document, without that person's express knowledge or consent."[452] Unintentionally reading such information is not a crime as long as it is not disclosed, used or stored, and as long as the information gleaned is promptly destroyed.[453] Finally, neither a governmental nor business entity may "remotely read an identification device using radio frequency identification technology for commercial purposes, unless that governmental or business entity, or one of their affiliates, is the same governmental or business entity that issued the identification device."[454] This is another provision targeted at protecting PII from skimming.

When it comes to disclosure of PII contained in public records under Washington's Public Records Act, a "person's 'right to privacy' . . . is invaded or violated only if disclosure of information about the person: (1) [w]ould be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public."[455] The code continues on to state that the "provisions of this chapter dealing with the right to privacy in certain public records do not create any right of privacy beyond those rights that are specified in this chapter as express exemptions from the public's right to inspect, examine, or copy public records.[456]

AV. *West Virginia*

1. *Electronic Monitoring & Eavesdropping*

West Virginia is a one-party consent state. More specifically:

> Recording a wire, oral, or electronic communication, or disclosing its contents, is not a violation of West Virginia law when the person recording is a party to the communication or has obtained consent from one of the

[451] *Id.* § 46.20.202 (2010).
[452] *Id.* § 9A.58.020.
[453] *Id.* § 9A.58.020(2)(c)(i)–(iii).
[454] *Id.* § 19.3.030.
[455] *Id.* § 42.56.050.
[456] *Id.*

> parties, so long as the recording is not accompanied by a criminal or tortious intent.[457]

As with the other rather standardized one-party consent statutes, West Virginia's wiretapping legislation allows for the authorization of a third party—uninvolved in the actual conversation—to intercept the communication.

2. *Miscellaneous Privacy Protection*

West Virginia law prohibits discrimination against employees who use tobacco products. The relevant statute states that it:

> [S]hall be unlawful for any employer, whether public or private, or the agent of such employer to refuse to hire any individual or to discharge any employee or otherwise to disadvantage or penalize any employee with respect to compensation, terms, conditions or privileges of employment solely because such individual uses tobacco products off the premises of the employer during nonworking hours.[458]

Certain non-profits whose purposes or objectives discourage the use of one or more tobacco products by the general public may discriminate in this respect.[459]

Employers are still allowed to offer, impose or have in effect "a health, disability or life insurance policy which makes distinctions between employees for type of coverage or price of coverage based upon the employee's use of tobacco products."[460] Finally, nothing in this lifestyle discrimination section "shall be construed to prohibit an employer from making available to smokers and other users of tobacco products, programs, free of charge or at reduced rates, which encourage the reduction or cessation of smoking or tobacco use."[461] This provision allows employers to be creative in encouraging their employees to quit smoking even though they cannot legally force them to do so.

---

[457] CAN WE TAPE?, *supra* note 41, at W. Va. (citing W. VA. CODE § 62-1D-3 (2010)).
[458] W. VA. CODE § 21-3-19 (2010).
[459] *See id.* § 21-3-19(b).
[460] *Id.* § 21-3-19(c) (stating, however, that "any differential premium rates charged to employees [through such a plan] must reflect differential costs to the employer [and that] the employer must provide employees with a statement delineating the differential rates used by its insurance carriers").
[461] *Id.* § 21-3-19(d).

AW. *Wisconsin*

1. *Electronic Monitoring & Eavesdropping*

Wisconsin's wiretapping statute allows one party to a conversation to monitor/intercept the communication itself or consent to a third party's interception of such conversation.[462] With this consent provision, Wisconsin joins the vast majority of states that have enacted one-party consent statutes similar to federal law.

2. *Miscellaneous Privacy Protection*

Wisconsin is one of the few states that prohibit the forced implantation of an RFID microchip.[463] A serious fine is attached to violations of this statute; more specifically, the code states that any "person who violates [this implantation prohibition] may be required to forfeit not more than [$]10,000. Each day of continued violation constitutes a separate offense."[464] Although no prison time is at stake, this large fine structure could lead to a huge total as long as an illegally placed RFID chip remains implanted in an individual.

Wisconsin state law also provides that

> [N]o employer . . . or other person may engage in any act of employment discrimination . . . against any individual on the basis of age, race, creed, color, disability, marital status, sex, national origin, ancestry, arrest record, conviction record, military service, *or use or nonuse of lawful products off the employers premises during nonworking hours.*[465]

The most interesting aspect of Wisconsin's lifestyle discrimination statute is that discrimination is prohibition for off-duty use *or nonuse* of lawful products. This "nonuse" clause would likely prohibit employers from forcing employees to take medicine to relieve the flu that is keeping the employee out of work. It will be interesting to track this provision to see if the "nonuse" clause rears its head in the case law.

Certain non-profit entities are exempt from this lifestyle discrimination prohibition. For example, the statute states that it is not discriminatory for employers in non-profit corporations to prohibit the off-duty use of a "lawful product [as long as such corporation] as one of its primary purposes

---

[462] WIS. STAT. § 968.31 (2010).
[463] *See id.* § 146.25.
[464] *Id.*
[465] *Id.* § 111.321 (emphasis added).

or objectives, discourages the general public from using a lawful product."[466] In addition, non-profit corporations may legally choose:

> [To] refuse to hire or employ an individual, to suspend or terminate the employment of an individual, or to discriminate against an individual in promotion, in compensation or in terms, conditions or privileges of employment, because that individual uses off the employers premises during nonworking hours a lawful product that the nonprofit corporation discourages the general public from using.[467]

AX. *Wyoming*

1. *Electronic Monitoring & Eavesdropping*

Wyoming law allows only one party to a conversation to intercept such communication or consent to its interception by a third party. More specifically, the state law reads that "no person shall intentionally . . . intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept any wire, oral or electronic communication."[468] This language is fairly standard among states with one party consent provisions and looks not only at interceptions but also at attempted interceptions and conspiracies to intercept. However, the one-party consent exemption allows any person to intercept an oral, wire or electronic communication "where the person is [either] a party to the communication or where one . . . of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act."[469] The most privacy protective aspect of this exception is the use of the word phrase "any criminal or tortious act." This type of restriction on the exception is as broad as can be found in any state wiretapping statute based on one-party consent.

2. *Miscellaneous Privacy Protection*

Wyoming law states that it is a discriminatory or unfair labor practice for an employer:

> [T]o require as a condition of employment that any employee or prospective employee use or refrain from using tobacco products outside the course of his

---

[466] *Id.* § 111.35.
[467] *Id.*
[468] WYO. STAT. ANN. § 7-3-702 (2010).
[469] *Id.* § 7-3-702(b)(iv).

> employment, or otherwise to discriminate against any person in matters of compensation or the terms, conditions or privileges of employment on the basis of use or nonuse of tobacco products outside the course of his employment.[470]

A relevant exception to this statute allows such discrimination as long as it is part of a "bona fide occupational qualification that a person not use tobacco products outside the workplace."[471] However, nothing in this section of the state code would "prohibit an employer from offering, imposing or having in effect a health, disability or life insurance policy distinguishing between employees for type or price of coverage based upon the use or nonuse of tobacco products" under most circumstances.[472] Considering the ever-increasing costs of health care and health-care deductibles, this provision might be used by employers to entice employees with a quasi-financial incentive to stop using tobacco products.

V. CONCLUSION

The American economy is going through some of the toughest times in recent memory. As businesses struggled and consumers found themselves in over their heads, the federal government immersed itself in the middle of colossal bailouts of major economic sectors. Problematically, as the economy begins to work itself back to stability and growth, serious problems linger. One of the most prominent of these problems stems from the potential for increasingly sophisticated technology operated by the government and the private sector to invade individual privacy. At the same time, consumers and businesses alike lack a clear national standard guiding the monitoring of persons and their personally identifying information.

State governments across the country continue to feel the heat from angry constituents and continually attempt to fill the breach by sporadically passing diverse privacy protection statutes. Some statutes deal with wiretapping, while others deal with employees' off-duty lifestyles, genetic testing, PII protection and RIFD tracking. The result has been a patchwork of privacy protection laws. Problematically, the patchwork of regulation that has been created has the potential to make the problem much worse. Businesses operating in interstate commerce must abide by potentially fifty different state laws. Employers, employees and consumers who move from state to state are likely to find themselves confused as to how these diverse laws protect them. At the end of the day, the best course to remedy the

---

[470] *Id.* § 27-9-105(a)(iv).
[471] *Id.*
[472] *Id.*

problem is for Congress to create a national standard. Until then, this Article has attempted to locate, categorize and evaluate relevant statutes across the fifty states. It is time for the federal government to end the state bailout when it comes to protecting individuals from invasion of privacy by sophisticated monitoring technology.